Privacy Concerns and Behavior on Social Networking Sites: An Empirical Examination

Divya Jain*[1], Ritu Saxena[2] & Abhishek Kapoor[3]
*[1]Assistant Professor, Jagannath International Management School, Kalkaji, New Delhi
[2]Associate Professor, Rukhmini Devi Institute of Advanced Studies, Rohini, Delhi
[3]Research Scholar, Amity Business School, Amity University, Noida

ABSTRACT

Purpose – The purpose of this paper is to propose and examine a privacy behaviour model in the context of Social networking factors (Indian scenario). The effects of key elements of SNS factors on perceived values of privacy behaviour were empirically determined.

Design/methodology/approach – SNS is conceptualized as a multi-dimensional construct including emotional privacy, social privacy, personal privacy, and value. The investigated socio demographic factors included, age, gender, ethnicity, education level, income level, and elements of SNS from which usually impacts the privacy behaviour. The primary data were gathered by a questionnaire survey of online users. Using 323 survey returns, factor analysis and Z test analysis were utilized for data analysis and hypothesis testing.

Findings – The proposed model was proven valid and the five value constructs cumulatively accounted for 70.2% of the variance in SNS for privacy behaviour. Social media parameters and Privacy scams significantly affected perceived social and emotional privacy behaviour. Online benefits and Legal structure significantly affected all perceived individual privacy concerns.

Practical implications – Incorporation of emotional privacy, social privacy, personal privacy, and value type information in developing SNS marketing strategies and promotional programs can help companies more effectively convey desired values of privacy to target consumers.

Originality/value – This empirical study responded to the need for better understanding of consumer privacy behaviour for SNS to support more effective product development and marketing. The knowledge gained from this study provides valuable insights for both academicians and industrial practitioners.

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

I. INTRODUCTION

The utilization of Social networking sites for informational and socialization motives is perhaps connected with the utilization of a mysterious profiles and clients inspired by web-based social networking's open measurements all the more effectively alter privacy settings (Xu, Luo, Carroll, & Rosson., 2011). The web-based social networking exhibited a constructive connection between the exposure of individual data and clients' number of companions and a pessimistic relationship between the utilization of privacy settings and the utilization of online networking to meet new individuals, proposing that privacy practices might be identified with social satisfactions (Culnan & Armstrong, 1999). The connection amongst security and sociality is very unpredictable. While positive connections exist between the utilization of privacy controls and social capital results, security demeanors may compel online networking exposure and contrarily affect the gathering of social capital advantages (Krasnova, Spiekermann, Koroleva, & Hildebrand, 2010). Clients see it important to trade individual data to acknowledge social objectives and achieve the social capital advantages that online networking offer and that the danger of unintended revelation is relieved by the social comfort for social administration (Boyd & Ellison, 2008).

Clients of web-based social networking show solid worries about security on the web, yet regularly don't participate in privacy ensuring practices, for example, modifying privacy controls, confining divulgence of geo-area data, or changing beginning privacy decisions after system development. The obvious logical inconsistency between security inclinations and privacy ensuring exercises has confused specialists, and has been regarded the security (Rosen, 2001). As a client focused approach, the utilizations and delights point of view gives knowledge to comprehend online networking use, as well as how web-based social networking use is impacted by privacy concerns and how its utilization may impact ordinary security. Security worries as being both social and institutional and identified with instructive exposure on informal community destinations) (Karyda, Gritzalis, Park, & Kokolaki, 2009). As the two essential zones for privacy concern, Information Control compares to the social parts of instructive exposure, while Power Loss relates dictator and institutional measurements. Personality Loss and Future Life of Information have likewise been perceived in earlier work, as "saw harm" and "saw probability" of mischief, predecessors to worry about security. Essentially, this examination distinguished the supremacy of Identity Loss and Future Life of Information as requested privacy concerns. This investigation additionally showed that security exercises take after a legitimate example that mirror various leveled levels of online movement (Li, Wang, Li, & Che, 2016).

Clients may go in their privacy practices, however this work additionally gives prove that clients shield their security at the same time at numerous levels. The worries about the utilization of character data and how substance will be dealt with later on may prompt more instrumental types of engagement with web-based social networking stages (Cho, Lee, & Chung, 2010). The online networking privacy is found in the utilization of Social Curation when web-based social networking is utilized for Communication or Escape. Relationship improvement from the shallow to more personal structures is frequently depicted as a procedure of self exposure in which the pressure of privacy control and the cordiality of the social setting highlight dominatingly (Christofides, Muise, & Desmarais, 2009). Social infiltration hypothesis and correspondence security administration hypothesis) underscore the pertinence of socially situated ways to deal with privacy that middle on revelation in unmediated connections. Interceded situations exhibiting those comparative sorts of limit control forms are practiced via web-based networking media stages and strengthening the hugeness of social methodologies in privacy direction forms. The online networking privacy recognized in this examination offers proof of how the security oddity may keep on surfacing (Awad & Krishnan, 2006). Propensity is identified with an absence of engagement of use level security administration devices. This is steady with how ongoing media utilize is portrayed by and large, deficient with regards to purposefulness or potentially thoughtfulness regarding the medium/message. The habituation crosses with privacy administration in ways that present the potential for disengagement between security concerns and privacy practices. Thusly, this prompts a proceeded with indication of the security conundrum, in spite of expanded understanding and modernity in online networking use (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 and protection administration in the reference of Social media destinations should be led in this way of research objective An organized survey had been intended to gather data from authentic Social media clients for reacting following exploration objectives:

- Are there critical privacy administration measures among Social media locales?
- To distinguish the components of privacy behaviour on Social media locales which influences the clients' disposition towards person to person communication destinations?

III. REVIEW OF LITERATURE

The expanded utilization of interpersonal Social networking sites has prompted expanded worries about clients' security not just as far as the information gathered and utilized by the association yet additionally in light of the conceivable effect of mass sharing of individual data on social relations (Akar & Topcu, 2011). Privacy concern can be named as the claim of people, gatherings, or foundations to decide for themselves when, how and to what degree data about them is imparted to others. It is accomplished through four primary techniques, the willful and brief withdrawal of a man from general society through physical or mental means, either in a condition of isolation or little gathering closeness or, when among vast gatherings, in a state of secrecy or hold (Bélanger & Crossler, 2011). The particular control of access to the self" and contends that protection is accomplished through the direction of social connection. In any case, regardless of many endeavors to make an amalgamation of the current writing around there (e.g., Parent), a bound together and basic record of security still can't seem to develop. Along these lines, later methodologies have tended to concentrate on the diverse measurements of protection. Different analysts recognize four measurements of protection and characterize it utilizing these measurements as the capacity to control and point of confinement physical, interactional, mental and instructive access to the self or one's gathering (Angulo, Hübne, Wästlund, & Pulls, 2012). This additionally mirrors the multidimensional idea of protection in her definition, which recognizes three measurements: educational, openness, and expressive security. At no time have security issues gone up against more noteworthy criticalness than as of late, as mechanical improvements have prompted the development of a 'data society' fit for get-together, putting away and dispersing expanding measures of information about people. While the basic idea of security isn't new, current mechanical headways have implied that protection concerns have advanced (Bryce & Klang, 2009). New ICTs have changed our capacity to gather, total, and offer information. Present day innovation has the capacity and power, especially in contrast with the pre PC time, to catch, store, and total, redistribute, and utilize information from singular clients. Researchers examined the lastingness and huge amount of the records held in such databases (Cranor, 2003). Taking note of that the proprietor of this data is frequently uninformed of, or if nothing else detached to, its stockpiling and usage, The resultant damages of security infringement might be both physical (e.g., real protection) and mental (e.g., dread of observation). The unapproved utilization of her picture by a kindred traveler brought about far reaching spread. Had it not been for the simplicity of dispersal and pursuit capacity offered by the Internet, this viral would not have been as broad, and not have brought about her leaving college, embarrassed. The Internet, apparently, has made such episodes significantly more typical and considerably less demanding for the regular individual to share in. Vitally, many individuals are additionally complicit in this disintegration of protection, specifically using Social networking sites to impart individual data to associates and showcasing associations (Dinev & Hart, 2006). Security concerns online have identified with internet business exchanges, strikingly misrepresentation, merchants' utilization of individual subtle elements, and client recognizable proof, yet with developing worry over what clients are posting on the web, the worry is never again related exclusively to such issues (Gauzente, 2004). In connection to SNS, this has a tendency to create around the point of character misrepresentation in light of clients' posting of data on their profiles or the Social networking sites itself permitting unhindered "default" get to. In spite of the fact that character misrepresentation, privacy extortion, and information stockpiling concerns are without a doubt disturbing, security is likewise hurt by clients' own conduct, for example, adolescents' pattern of "sexting" each other, digital tormenting and the failure to control one's social circles on SNS (Gudura, Cranor, & Arjula, 2006). Protection can be seen from the point of view of control. Regardless of whether it is control over individual information, the decision to unveil information, the physical nearness of others, the quantity of others display in exposure, or picking which individual to talk about and share issues with, control is integral to looking after security (Hiller, Smith, & Bélanger, 2002). Specifically, Social cooperation with our condition, proposed the idea of individual, dyadic, and a mass limits for controlling security and divulgence. In day by day disconnected life, these limits have a tendency to be self-evident. In any case, controlling these limits and the data stream between them in a SNS domain can demonstrate troublesome because of the diverse utilization of the term "companion". In Social networking sites, the term "companion" is regularly used to indicate any number of potential relationship ties (Hong & Thong, 2013). The need to control the stream of individual data to various sorts of relationship attach is integral to our social world. We permit certain more nitty gritty, insinuate parts of ourselves to be discharged or imparted to another as a major aspect of a private obligation of closeness, though we discharge less data to the individuals who we to hold a lesser cozy association with. For instance, we may impart diverse data to a cozy accomplice than with a parent. In choosing which components of one's identity and individual data to discharge to different kinds of relationship, the centrality of each might be helpful in deciding how private data . (Krasnova, Gunther, Spikermann, & Koroleva, 2009)portray the centrality of identity as like unique and developing layers of an onion. The centrality of people inside an informal community has been proposed to identify with levels of expected security. In the event that individual data is taken by another and spread to associations facilitate from the person than would sensibly be normal by their own methods and close companion aggregate then it is contended as an infringement of protection. In online collaboration, for example, a SNS, the refinement between who can see, get, and utilize different bits of our information or picture ends up plainly obscured. Virtuality makes a man administration issue (Nissenbaum, 2004). By including various kinds of "ties" to our "companions" list on, for instance, Facebook, it winds up noticeably hard to oversee access and imparting to various individuals and sorts of "companion" (Xie, Teo, & Wan, 2006). For instance, photographs of intoxicated trips might be readily imparted to companions, yet would they say they are so enthusiastically imparted to family, work partners, or even potential businesses? On the web, unless controlled and oversaw through regularly entangled protection settings, everyone in the "companions" rundown can get to these photographs. Hence, overseeing social circles ends up noticeably confounded, and such entanglements and unexpected conditions may prompt security hurts. Issues of protection on SNS can rely upon the site utilized and the client's site settings and individual security inclinations (Rotenberg & Scott, 2015). For example, Facebook gives the capacity to make an unmistakable individual profile including photos, main residence, date of birth, relationship status, and email address that is then transparently accessible to possibly obscure others. Besides, unless protection settings are tweaked, clients might be ignorant to whom they are dispersing data. Arrival of individual and private data may cause extra security issues including phishing, data spillage, and stalking. Interpersonal organization destinations that don't transparently give individual points of interest are not excluded from protection issues, possibly sufficiently giving data to recognize the client, for example, by a photo normal with different SNS of course (Sheehan, 2002). Late changes to the security settings of Facebook have additionally muddled this issue by making much data (e.g., photos, arrangements of "companions") open to everybody of course for the lion's share of clients (Solove, 2001).

IV. RESEARCH METHODOLOGY

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

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

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

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 were employed 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 most impactful 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

V. DATA ANALYSIS

Exploratory Factor Analysis: Principal component method with varimax rotations was used to reduce the proportions 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. Principal component analysis employed to measure the degree of variability in the variables. The degree of variability calculated from the initial value [=1], variables with extraction value more 0.5 would be considered acceptable for 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 factor extraction. It was found that total five factors with (Eigen value >1) accounts for 70.2% variance in all variables considered 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 the variables.

V1= Information sold
V2= Privacy system
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 leaked
V17 Code of conduct for data
V18= Marketing of media
V19= Concessions
V20= Identity theft
V21= Rewards

Exhibit 5

Detailed evaluation of factor analysis results as shown in Exhibit 5 and Exhibit 6 above, led to identification of five rational factors, which were named subsequently on the basis of variables which were grouped together under different factors.

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**

VI. 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 behaviour on social media sites.*
H2: *Privacy scams on social media sites have a direct influence on a user's intent with respect privacy behaviour on social media sites.*
H3: *Online benefits to the users have a direct influence on a user's intent with respect privacy behaviour on social media sites.*
H4: *Legal structure has a direct influence on a user's intent with respect privacy behaviour on social media sites.*
H5: *User's attitude has a direct influence on a user's intent with respect privacy behaviour on social media sites.*

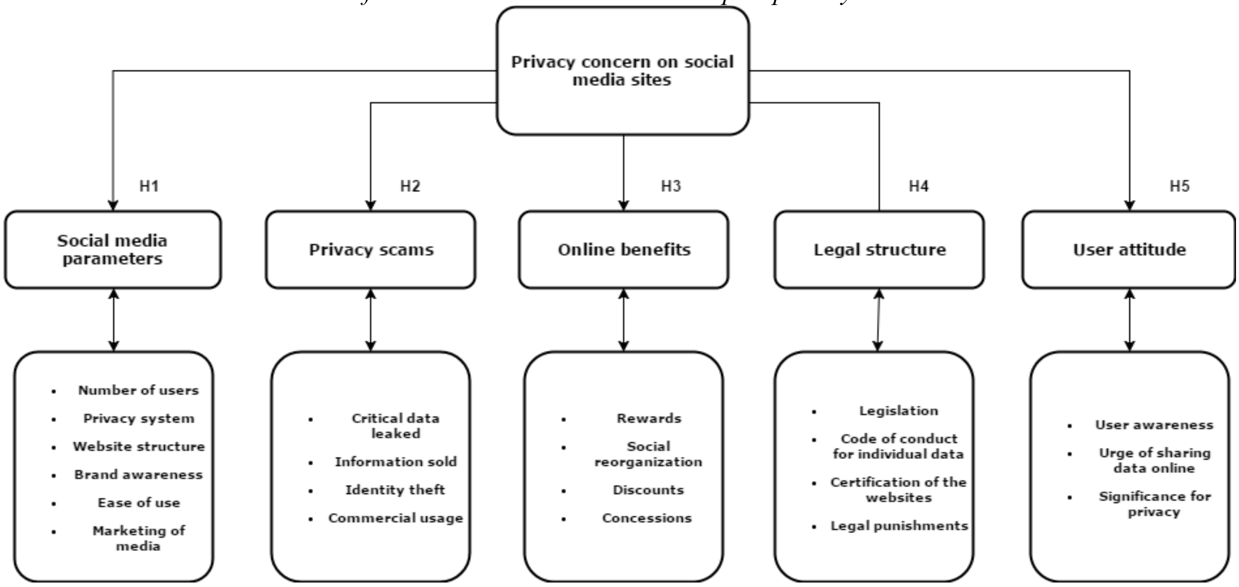

Figure 1 Proposed model of the study

Multiple regression analysis

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*

VII. 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 by using 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, Brand awareness, Ease of use and Marketing of media. *Factor 2* Privacy scam consists of variables Critical information leaked, Information sold, Identity theft and Commercial usage. *Factor 3* Online benefit consists of variables Discounts, Social recognition, Concessions and Rewards. *Factor 4* Legal structure consists of variables Legislation, Code of conduct for data, Certification of sites and Legal punishment. *Factor 5* User attitude consists of variables User awareness, Urge to share data online and Significance for piracy. The results of data analysis are segmented into two sections. Section 1 consist of descriptive statistics of demographic and search engine profile of the respondents and the majority of the respondents between the age of 20-25 years with graduate level of education use Google as there prominent search engine for mostly 15 - 60 minutes in order to obtain updates and information. Section 2 on other hand consists of Statistical and Hypothetical analysis of the identified variables. Privacy behaviour with respect to SNS *(F value* 22.19 *and p value <.0001)* has significant impact on the consumers. The most prominent elements of privacy behaviour identified in the research is it helps to social media parameters *(p value =-0.619)*, enhances the privacy behaviour of the user *(p value* = -0.15*)* followed by other factors i.e. Privacy scams.

VIII. CONCLUSION

Based on the survey results and theoretical comparative literature review, companies need to be aware of the implications of privacy behaviour in SNS. There is growing evidence to suggest that younger people are more concern for privacy than was typical a generation ago. This provides opportunities and challenges for SNS to focus on the grey market.

All of these conditions provide important insights into new patterns of consumer privacy behaviour for SNS to respond. The trend for younger consumers to have an increasing influence on the market place shows no signs of slowing 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 to marketing that reflects rather than compromises their key values. Limited research has been undertaken to compare factors that affect why young users concern about privacy, how they behave, and what they set as their privacy, in relation to their age, gender and nationality. This research goes some way to address some of these concerns and begins the process of identifying key factors that need to be considered by SNS administrations and marketers.

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

IX. REFERENCES

[1] Akar, E., & Topcu, B. (2011). An examination of the factors influencing consumers' attitudes toward social media marketing. Journal of Internet Commerce , 10 (1), 35-67.

[2] Angulo, J., Hübne, S. F., Wästlund, E., & Pulls, T. (2012). Towards usable privacy policy display and management. Information Management & Computer Security , 20 (1), 4-17.

[3] Awad, N., & Krishnan, M. (2006). The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization. Management Information Systems Quarterly , 30 (1), 13-28.

[4] Bélanger, F., & Crossler, R. (2011). Privacy in the digital age: a review of information privacy research in information systems",research in information systems. Management Information Systems Quarterly , 35 (3), 1017-1041.

[5] Boyd, D. M., & Ellison, N. B. (2008). Social networking sites:Defination, history and scholarship. Journal of Computer Mediated Communication , 13 (1), 210-230.

[6] Bryce, J., & Klang, M. (2009). Young people, disclosure of personal information and online privacy: control, choice and consequences. Information Security Technical Report , 14 (3), 160-166.

[7] Casado, N. S., Navarro, J. G., Wensley, A., & Solano, E. T. (2016). Social networking sites as a learning tool. The Learning Organization , 23 (1), 23 - 42.

[8] Cho, H., Lee, J., & Chung, S. (2010). Optimistic bias about online privacy risks: testing the moderating effects of perceived controllability and prior experience. Computers in Human Behavior , 26 (5), 987-995.

[9] Christofides, E., Muise, A., & Desmarais, S. (2009). Information disclosure and control on facebook: are they two sides of the same coin or two different processes? Cyber Psychology & Behavior , 12 (3), 341-345.

[10] Cranor, L. ,. (2003). P3P: making privacy policies more useful. IEEE Security & Privacy , 1 (6), 50-55.

[11] Culnan, M., & Armstrong, P. (1999). Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation. Organization Science , 10 (1), 104-115.

[12] Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. Information Systems Research , 17 (1), 61-80.

[13] Gauzente, C. (2004). Web merchants' privacy and security statements: how reassuring are they for consumers? A two-sided approach. Journal of Electronic Commerce Research , 5 (3), 181-198.

[14] Gudura, P., Cranor, L., & Arjula, M. (2006). User interfaces for privacy agents. ACM Transactions on Computer-Human Interaction , 13 (2), 135-178.

[15] Hiller, J., Smith, W., & Bélanger, F. (2002). Trust worthiness in electronic commerce: the role of privacy, security, and site attributes. Journal of Strategic Information Systems , 11 (3), 245-270.

[16] Hong, W., & Thong, J. (2013). Internet privacy concerns: an integrated conceptualization and four empirical studies. Management Information Systems Quarterly , 37 (1), 275-298.

[17] Karyda, M., Gritzalis, S., Park, J., & Kokolaki, S. (2009). Privacy and fair information practices in ubiquitous environments: research challenges and future directions. Internet Research , 19 (2), 194-208.

[18] Krasnova, H., Gunther, O., Spikermann, S., & Koroleva, K. (2009). Privacy concerns and identity in online social networks. Identity in the Information Society , 2 (1), 39-63.

[19] Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks:why we disclose. Journal of Information Technology , 25 (6), 109-125.

[20] Li, K., Wang, X., Li, K., & Che, J. (2016). Information privacy disclosure on social network sites . Nankai Business Review International , 7 (3), 282-300.

[21] Nissenbaum, H. (2004). Privacy as contextual integrity. Washington Law Review , 79 (1), 101-139.

[22] Rosen, J. (2001). Out of context: the purposes of privacy. Social Research , 68 (1), 209-220.

[23] Rotenberg, M., & Scott, J. (2015). Privacy in the Modern Age : The Search for Solutions. New York: The New Press.

[24] Sheehan, K. (2002). Toward a typology or internet users and online privacy concerns. Information Society , 18 (1), 21-32.

[25] Solove, D. (2001). Privacy and power: computer databases and metaphors for information privacy. Stanford Law Review , 53 (6), 1393-1462.

[26] Xie, E., Teo, 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.

[27] Xu, H., Luo, X., Carroll, J., & Rosson., M. (2011). The personalization privacy paradox: an exploratory study of decision making process for location-aware marketing. Decision Support Systems , 51 (1), 42-52.