ISSN: 2394-7659
IMPACT FACTOR- 2.789

International Journal of Engineering Researches and Management Studies

VALUE FOR PRIVACY ON SOCIAL MEDIA SITES WITH SPECIAL REFERENCE TO YOUNG USERS

Dr. Himani Sharma[*1] & Ravneet Singh Bhandari[2]
[*1]Associate professor Associate Professor, Marketing & Sales, Amity Business School, Amity University, Noida
[2]Research Scholar, Amity Business School, Amity University, Noida

ABSTRACT
This paper inspects the impact of interactive social media communication network on young users for the value of privacy components associated to their individual personality. The study also considers the impact of numbers of additional factors for example usage (access by users, length of usage by users, log on frequency of the users, log on duration and profile update incidences of users), demographic factors (age, gender, education of the users) and factors on young user' attitudes for value of privacy towards social media marketing communications. The research was directed via a self-administered questionnaire, which were distributed to around 323 social media users' age between 14 -26 years from the National Capital Region (NCR) of Delhi in India. A generalized exploratory factor analysis was used to club the number of variables into factors for more relevant and authentic data analysis and summed linear modeling was employed for statistical hypothetical testing, the collected data from the respondents was coded in R for the mentioned statistical analysis. The review discovered that there is high level of concern for privacy on each attitude component among youngsters on social media marketing communications, The results also uncovered that young users who used social media for long time periods; refreshed their profiles frequently, displayed the most positive attitudinal reactions for the value and concern for the privacy on the social media marketing communications. Social media administrators should consider utilizing and adapting high standards with respect to the privacy settings for the users, their strategies should based on the making the social media sites more user friendly and protective with respect to the personal and confidential information of the users.

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

1. INTRODUCTION

Statements in regards to social networking sites penetration and its significance for business are euphoric. Social networks are evolving fast as with the rapid development of the technology. They are turning to be the one-stop search for all online discourse needs (Arora & Predmore, 2013). A present scenario: Facebook the most widespread online networking website in the contemporary digital world holds around 1.79 billion monthly users worldwide. (Diephay, 2016).

Various services identified with social media sites enable users a space to share proficient as well personal data (Bhandari & Sharma, 2017). An expansive definition of social media as defined by the digital media experts "These online administrations empower people to make a semi-open or open profile inside a limited framework, the likelihood to build a list of contacts of other social media users with whom they share an association and in addition to review their individual social media profile which are made by others inside the respective framework" (Boyd & Ellison, 2008). Presently, several social media sites are among visited web sites universally. In this manner, users offer their respective profiles as well as further information about themselves , for instance comprising of interests, individual values and standards, information about friends, school and out-of-school data, , therapeutic and most likely monetary data and in addition data about their working environment (Li, Wang, Li, & Che, 2016). Social media sites uncover bits of knowledge about users' preferences, considerations and favored music, moreover nowadays users also alludes to geo tagging as a new trend to include graphical data of users (Bryce & Klang, 2009)

In view of many recent publicized privacy violation conveyed by media, data protection with respect to social media sites has turned into a general discussed issue. Moreover, researches demonstrate that most social

ISSN: 2394-7659
IMPACT FACTOR- 2.789

International Journal of Engineering Researches and Management Studies

networking sites offer little clarification about the decisions users have to take and the effects of their choices, so they are made a request to create their own techniques to deal with their privacy needs (Casado, Navarro, Wensley, & Solano, 2016). Standard protection settings on most social media sites the individual information and utilization behaviour are stored, investigated, and transmitted to third parties so that the tastes of the users end up noticeably known to marketers that are permitted to target users with customized marketing strategies (Bélanger & Crossler, 2011). Such data is utilized as a imperative way for offers and promoting methodologies, by insurance companies and media organizations, data merchants, monetary surveillance or cybercrime exercises (Hong & Thong, 2013). More in particular, privacy related dangers could be founded on computerized dossiers of individual data for instance dangers of coercing or harm of the reputation of profile holders (Xie, Teo, & Wan, 2006). In this way, character related dangers may happen through phishing assaults, data spillage, and profile crouching through identity fraud, and social dangers can be based on stalking and corporate secret activities (Xu, Luo, Carroll, & Rosson., 2011). From one perspective, abundant user information on social networking sites illustrate extraordinary opportunities to users, for instance in order to connect with associates. Then again, an intentional and progressive loss of security of the individual may happen. Cases might be identity extortion ,the inability to control one's social circle, online badgering, digital stalking (in view of the accessibility of individual data on social media sites, digital mobbing, digital harassing (for instance, coursing false bits of gossip about a user or posting unfavorable messages on one's client site (Gauzente, 2004). Hence, beside individually seen positive aspects of social media sites for users, their data is perhaps being used for above-mentioned partly erratic and miscellaneous purposes (Sheehan, 2002).

Privacy management

Privacy management aims at creating privacy-enhancing character management systems for technically enforcing user control and information self-control. A critical essential for supporting clients' control in this setting is to exhibit straightforward and reasonable protection arrangements. For accomplishing better transparency, privacy settings enables users to characterize and adjust their protection inclinations proclaiming under which conditions they might want to discharge what sorts of information (Cranor, 2003). Privacy settings also have the capacity of contrasting the users' inclinations with the privacy strategies of social media sites, so users can be educated about the degree to which their security inclinations will be fulfilled. Though, for ordinary PC users, characterizing and adjusting their protection inclinations for legitimately ensuring their protection online are complex and error-prone tasks inclined undertakings which generally require some level of ability on essential lawful protection ideas and standards. Moreover, it is not sensible to accept that users will spend their time and exertion on arranging privacy inclinations, since privacy and protection assurance are rarely the users' primary tasks. In a disconnected world individuals deal with their protection inclinations pretty much naturally, making oblivious decisions about the snippets of data they uncover as per the settings in which they end up in at specific circumstances. For instance, an individual instinctively knows which data is appropriate to impart to his Doctor, and which would be unseemly to impart to her partners at work (Gudura, Cranor, & Arjula, 2006). Accordingly, the challenge lies in how to decipher that intuitive comprehension and administration of individual privacy to the digital world. For streamlining the administration of privacy inclinations, various researchers have proposed the novel approach of giving users a predefined standard protection settings which can be modified as per requirements (i.e. can be changed and spared as an on the web exchange happens) and to help them right now of choosing affirming traits that check their identity. For making privacy strategies more reasonable and straightforward, legislative bodies have prescribed giving policy in a multi-layered arrangement. A short security notice on the top layer must offer people the center data required, which incorporates at slightest the character of the specialist organization and the motivation behind information processing. Furthermore, a reasonable sign must be offered with reference to how the individual can get to alternate layers introducing the extra data required, for example, data on regardless of whether the individual is obliged to answer to the social media service provider's inquiries, and on the lawful privileges of the information subject on the social media sites (Angulo, Hübne, Wästlund, & Pulls, 2012).

2. OBJECTIVES OF THE STUDY

With orientation to the above information it could be detected examination regarding concern for privacy and privacy management in the reference of Social media sites need to be conducted therefore A structured questionnaire had been designed to collect information from actual Social media users for responding following research objectives:

ISSN: 2394-7659
IMPACT FACTOR- 2.789

IJERMS

International Journal of Engineering Researches and Management Studies

- Are there significant privacy management measures among Social media sites?
- To identify the elements of privacy concern on Social media sites which affects the users' attitude towards social networking sites.

3. REVIEW OF LITERATURE

Academic research about social media sites demonstrates that the availability of the tremendous amount of information accessible on social media sites evolved them as data warehouses. As a matter of first importance we need to understand that how to characterize privacy with respect to each individual user and what aspects appear to be relevant. As individuals utilize the opportunity improving measurements of the web, as they communicate also, take part in self-advancement, they might be obliging the flexibility and self-improvement of others – and even of themselves (Awad & Krishnan, 2006). Privacy can be something alluding to "lost", "attacked", "meddled with", "abused", "lessened", "ruptured", and others; each of these allegories allude to existing privacy concepts and applied systems. Few existing and extensively talked about philosophical privacy perspectives: the privilege to be isolated, restricted access to the self, protection as mystery and control over individual data (identity, closeness, and protection as group idea). Privacy includes a man's entitlement to control the spread his/her individual data. However, privacy still is by all accounts "a general idea, incorporating (in addition to other things) flexibility of thought, control over individual data, flexibility from online observation, security of one's online reputation, and assurance from online tracking down and cross examinations . Most important aspect, specifically control over data around oneself, is one of the fundamental issues esteeming privacy (Hiller, Smith, & Bélanger, 2002). Distinctive variants of control speculations of instructive privacy gives a connection amongst privacy and mystery and depicts privacy as the claim of people to decide for themselves when, how, furthermore, to what degree data about them is imparted to others (Cho, Lee, & Chung, 2010).

Additionally, in a more recent research articles, individual privacy is said to be based on the consistent changing of person's needs as far as various situational occasions and life-cycle progress. Privacy is seen as a dynamic and rationalization limit control handle: the ecological setting (for illustration distinctive data architectures on social media sites influences social privacy behaviour (Krasnova, Gunther, Spikermann, & Koroleva, 2009). In different words, additionally the privacy condition on social media sites impacts users' security activities. Privacy as the person's capacity to control the course of data identifying with him, and association between our capacity to control who approaches data about us and our capacity to make and keep up various sorts of connections (Akar & Topcu, 2011). In general, many of the above mentioned issues must be viewed as a sort of individual flexibility inside a confined territory (Nissenbaum, 2004). Referring to online social systems one may pose a few inquiries: to start with, is it suspicious to expect having far reaching control over individual data given on social media sites? Or, then again is it control over the availability of information? Which information in detail? Do we choose and adjust pros and cons normally when we uncover content on social media sites? Additionally raises the question on the contrary that users can uncover gigantic data on social media sites and still have privacy in light of a broad control over one's confidential and personal data as a potential state of our protection (Rosen, 2001).

In online social media communities, people (typically) can choose what individual data is accessible to people in general. In addition, information may lead the user straightforwardly to another user. So, informational privacy of an individual user can overlap with ease of access information when the acquisition of information additionally involves gaining access to a person confidential data (Solove, 2001). An advance aspect can be seen in the field of new potentials of insidious data combination on social media sites with data on other relevant platforms for instance Banks. Such availability of data decreases the ability of individuals' control over information about themselves. For example, current research focuses on the role of ubiquitous environments as a new privacy-related context and claims for so-called "fair information practices" aiming at a protection of individuals' private data. Such accessibility of data diminishes the capacity of people's control over data about themselves (Dinev & Hart, 2006). Existing researches focuses on the role of ubiquitous environments as a standard privacy related setting and claims for "reasonable data practices" going for an assurance of user's private data. A couple of aspects of reasonable data practices can be reconsidered and adjusted for online social communication situations; these are: The need to help users with particular data about their own information (Rotenberg & Scott, 2015). Users ought to have the likelihood to make information based and free decisions with respect to collection and the particular utilization of their respective data.. Consequently, social media sites

ISSN: 2394-7659
IMPACT FACTOR- 2.789

IJERMS

International Journal of Engineering Researches and Management Studies

administrators should be welcomed to the platforms for instance on their privacy approaches and standard privacy settings (Karyda, Gritzalis, Park, & Kokolaki, 2009). One open platform with potential for benefits for both social media administrators and users might help in development and implementation of a standardized and transparent designed privacy model (Krasnova, Spiekermann, Koroleva, & Hildebrand, 2010).

The utilization and control of data quality on social media sites requires a systematic treatment of both administrators as well as users, for example due to specific odds of users' friends on social media sites (Christofides, Muise, & Desmarais, 2009). Diverse nations have distinctive strategies and standards, specific laws, parts of self-course like the usage of privacy enhancing settings. In this way, social media service providers administering individual information of users should absolutely consider their individual security accounts and related approval needs (Hope, 2007). In rundown, new (multidisciplinary) security approaches in more progressed and "unavoidable" conditions need to concentrate their attempts on privacy protecting requirements that the person as user can set autonomous from any other individual, including standardized functionalities for data affirmation frameworks and restriction. Each one of these attempts should incite a more authentic social media use (Culnan & Armstrong, 1999).

4. RESEARCH METHODOLOGY

An examination study was utilized to gather information keeping in mind the end goal to assess the level of privacy concern among social media users, and to test the research hypotheses outlined previously. This study aimed to investigate the impact of privacy concern on users' acceptance of social media sites in natural environment. A survey questionnaire was developed to measure each of the constructs contained in our exploration research model. Measurement of the variables for the constructs in the research model was adapted from the review of the literature. Each variable was measured on a five-point Likert scale where 1 means "strongly disagree" and 5 means "strongly agree". A pilot study was used to ensure that the examined variables are significant to the users of social media sites. Based on the results from the pilot study, modifications were made to the questionnaire. The concluded questionnaire was then circulated to young users. In total, 357 survey questionnaires were returned from the survey respondents. After screening out incomplete responses, the survey yielded 323 usable responses. Exhibit 1 and Exhibit 2 provide the summary of respondents' demographic information as well as their social media sites usage patterns.

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 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.

ISSN: 2394-7659
IMPACT FACTOR- 2.789

IJERMS

International Journal of Engineering Researches and Management Studies

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

5. 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.

ISSN: 2394-7659
IMPACT FACTOR- 2.789

IJERMS

International Journal of Engineering Researches and Management Studies

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 analysis* *Extraction method= Principal Component*

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.

Correlation matrix

	V1*	V2*	V3*	V4*	V5*	V6*	V7*	V8*	V9*	V10*	V11*	V12*	V13*	V14*	V15*	V16*	V17*	V18*	V19*	V20*	V21*
V1*	1.00	0.31	0.19	0.19	0.13	0.11	0.19	0.36	0.16	0.19	0.33	0.11	0.16	0.06	-0.1	0.11	0.19	0.36	0.16	0.19	0.16
V1*	0.31	1.00	0.69	0.13	0.33	0.36	0.66	0.16	0.19	0.19	0.16	0.19	0.03	0.11	0.09	0.36	0.66	0.16	0.19	0.19	0.19
V3*	0.19	0.69	1.00	0.36	0.39	0.19	0.60	0.16	0.33	0.30	0.36	0.16	0.16	0.13	0.11	0.19	0.60	0.16	0.33	0.30	0.33
V4*	0.19	0.13	0.36	1.00	0.63	0.61	0.33	0.16	0.33	0.16	0.61	0.36	0.16	0.11	0.11	0.61	0.33	0.16	0.33	0.16	0.33
V5*	0.13	0.33	0.39	0.63	1.00	0.69	0.61	0.33	0.63	0.61	0.66	0.66	0.31	0.61	0.79	0.69	0.61	0.33	0.63	0.61	0.63
V6*	0.11	0.36	0.19	0.61	0.69	1.00	0.63	0.11	0.66	0.36	0.16	0.66	0.11	0.31	0.33	0.65	0.63	0.11	0.66	0.36	0.66
V7*	0.19	0.66	0.60	0.33	0.61	0.63	1.00	0.30	0.61	0.66	0.69	0.63	0.16	0.61	0.39	0.63	0.57	0.30	0.61	0.66	0.61
V8*	0.36	0.16	0.16	0.16	0.33	0.11	0.30	1.00	0.61	0.33	0.60	0.66	0.36	0.33	0.39	0.11	0.30	0.46	0.61	0.33	0.61
V9*	0.16	0.19	0.33	0.33	0.63	0.66	0.61	0.61	1.00	0.61	0.63	0.69	0.36	0.61	0.61	0.66	0.61	0.61	0.52	0.61	1.00
V10*	0.19	0.19	0.30	0.16	0.61	0.36	0.66	0.33	0.61	1.00	0.63	0.63	0.13	0.36	0.46	0.36	0.66	0.33	0.61	0.67	0.61
V11*	0.33	0.16	0.36	0.61	0.66	0.16	0.69	0.60	0.63	0.63	1.00	0.66	0.61	0.76	0.49	0.16	0.69	0.60	0.63	0.63	0.63
V12*	0.11	0.19	0.16	0.36	0.66	0.66	0.63	0.66	0.69	0.63	0.66	1.00	0.11	0.63	0.61	0.66	0.63	0.66	0.69	0.63	0.69
V13*	0.16	0.03	0.16	0.16	0.31	0.11	0.16	0.36	0.36	0.13	0.61	0.11	1.00	0.13	0.61	0.11	0.16	0.36	0.36	0.13	0.36
V14*	0.06	0.11	0.13	0.11	0.61	0.31	0.61	0.33	0.61	0.36	0.36	0.63	0.13	1.00	0.61	0.31	0.61	0.33	0.61	0.36	0.61
V15*	-0.1	0.09	0.11	0.11	0.69	0.33	0.39	0.39	0.61	0.56	0.49	0.61	0.61	0.61	1.00	0.33	0.39	0.39	0.61	0.56	0.61
V16*	0.61	0.33	0.16	0.31	0.19	0.19	0.13	0.11	0.19	0.36	0.16	0.19	0.33	0.11	0.16	1.00	0.13	0.11	0.19	0.36	0.19
V17*	0.66	0.36	0.61	0.56	0.79	0.13	0.33	0.36	0.66	0.16	0.19	0.19	0.16	0.19	0.03	0.13	1.00	0.36	0.66	0.16	0.66
V18*	0.69	0.66	0.36	0.69	0.16	0.36	0.39	0.19	0.60	0.16	0.33	0.30	0.36	0.16	0.16	0.36	0.39	1.00	0.60	0.16	0.60
V19*	0.63	0.16	0.66	0.13	0.36	0.34	0.63	0.61	0.33	0.16	0.33	0.16	0.61	0.36	0.16	0.34	0.63	0.61	1.00	0.16	0.33
V20*	0.16	0.19	0.33	0.33	0.39	0.63	0.46	0.69	0.61	0.33	0.63	0.61	0.66	0.76	0.31	0.63	0.46	0.69	0.61	1.00	0.61
V21*	0.61	0.19	0.61	0.36	0.19	0.61	0.69	0.39	0.63	0.11	0.66	0.36	0.16	0.56	0.11	0.61	0.69	0.39	0.63	0.11	1.00

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 5

ISSN: 2394-7659
IMPACT FACTOR- 2.789

IJERMS

International Journal of Engineering Researches and Management Studies

Exhibit 6 **Eigenvalues of the Correlation Matrix: Total = 21 Average = 1**

	Eigenvalue	Difference	Proportion	Cumulative
1	7.16439432	4.45814556	0.341161634	0.192630871
2	2.70624876	0.73642526	0.128868989	0.470030623
3	1.9698235	0.10914451	0.093801119	0.563831742
4	1.86067899	0.81301154	0.088603761	0.652435503
5	1.04766745	0.25287846	0.049888926	0.70232443
6	0.79478899	0.18071121	0.037847095	0.740171524
7	0.61407778	0.07192100	0.029241799	0.769413323
8	0.54415678	0.00123652	0.025816990	0.795230313
9	0.5433933	0.03579341	0.025971110	0.821201422
10	0.50759989	0.03994095	0.024171423	0.845372846
11	0.46765894	0.01421682	0.022269473	0.867642319
12	0.45344212	0.04658965	0.021592482	0.889234801
13	0.40685247	0.06997396	0.019373927	0.908608728
14	0.33687851	0.01664920	0.016041834	0.924650562
15	0.32022931	0.07922654	0.015249015	0.939899577
16	0.24100277	0.00591832	0.011476322	0.951375899
17	0.23508445	0.01482879	0.011194498	0.962570397
18	0.22025566	0.00310862	0.010488365	0.973058761
19	0.21714704	0.01684904	0.010340335	0.983399097
20	0.200298	0.05197703	0.00953800	0.992937097
21	0.14832097		0.007062903	1.00000000

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**	

ISSN: 2394-7659
IMPACT FACTOR- 2.789

IJERMS

International Journal of Engineering Researches and Management Studies

User awareness	**0.77341**
Urge to share data online	**0.68432**
Significance for piracy	**0.59543**

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.

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 concern on social media sites.*

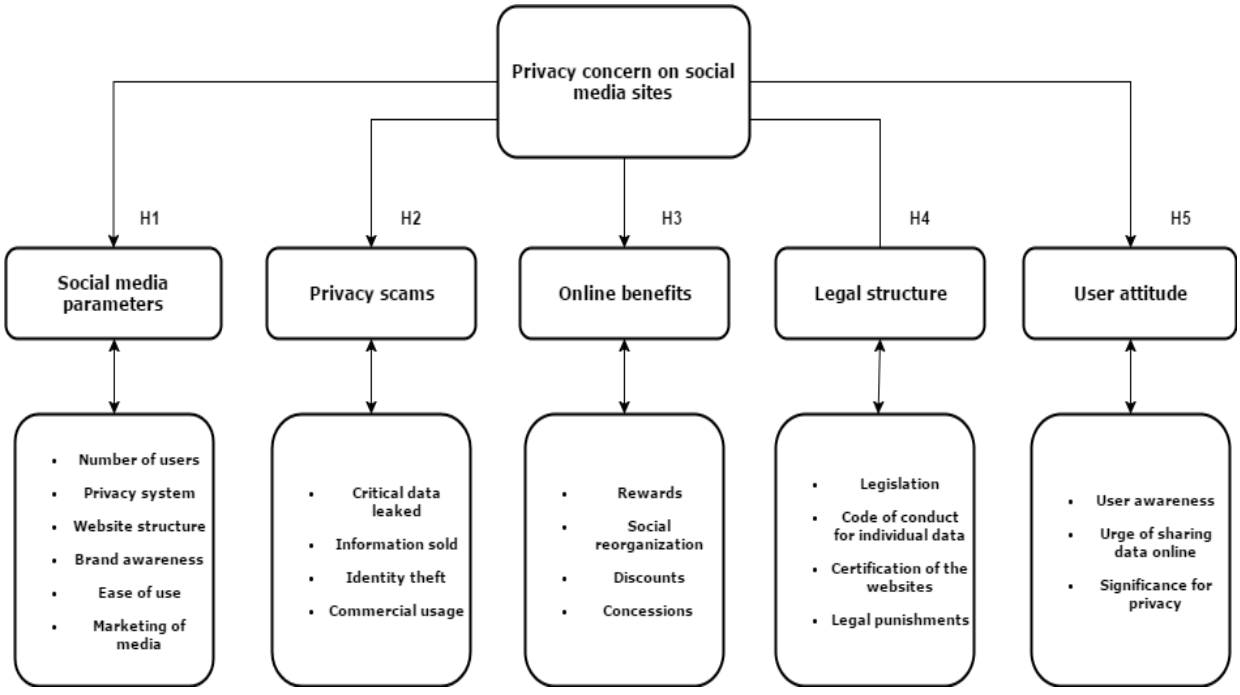
H2: *Privacy scams on social media sites have a direct influence on a user's intent with respect privacy concern on social media sites.*

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

H4: *Legal structure has a direct influence on a user's intent with respect privacy concern on social media sites.*

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

Based on the hypotheses described above, the proposed model of the study is demonstrated in the Exhibit 7.



ISSN: 2394-7659
IMPACT FACTOR- 2.789

IJERMS

International Journal of Engineering Researches and Management Studies

Exhibit 7 ***The proposed model of the study***

Multiple regression analysis

Variable	DF	Parameter Estimate	Standard Error	t Value	Pr > |t|
Intercept	1	1.44805	0.39727	3.65	0.0003
Social media site parameters	1	-0.57522	0.09293	-6.19	<.0001
Privacy scams on the website	1	-0.01890	0.12204	-0.15	0.0877
Online benefits	1	-0.01823	0.06266	-0.29	0.0713
Legal structure	1	0.38823	0.08940	4.34	0.0367
User's attitude	1	1.44805	0.39727	3.65	0.0106

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

Analysis of Variance

Source	*DF*	*Sum of Squares*	*Mean Square*	*F Value*	*Pr > F*
Model	5	230.75308	23.07531	27.19	<.0001
Error	312	245.24692	0.84861	***Depd. Mean*** 2.36000	**R-Square** 0.5524
Corrected Total	317	476.00000	***Root MSE*** 0.92120	***Coeff Var*** 43.29225	**Adj. R-Sq** 0.5458

Exhibit 9 *Results for privacy concern based on the identified variables*

Predicted (Privacy concern on social media sites) = -1.44805+ (-0.57522*Social media site parameters) + (-0.01890* Privacy scams on the website) + (-0.01823* Online benefits) + (0.38823* Legal structure) + (1.44805* User attitude)

6. CONCLUSION

The contribution of this paper is manifold. First, it has presented a current literature review of social media sites research highlighting diverse information privacy concern issues. The review has suggested several main factors: Privacy scams on the social media sites and benefits provided by these social media sites to be a current trend with privacy concern purposes; young adults seem to be more concerned about potential privacy threats than other users; and policy makers should be alarmed by a large part of users who underestimate risks of their information privacy on social media sites. However, it has to been observed that currently most social media service providers perhaps making money by selling users' data to third parties. Multidimensional privacy policies have to be considered in the dynamic digital environments. Systematic strategies has to be developed for privacy safeguarding, may include special functionalities for data protection mechanisms and self controllable privacy settings should be designed for more proper social media sites usage.

Utilizing data gathered from the survey, researcher tried the exploration models. Our information from examination shows that the immediate impact of privacy concern on behavior. While some earlier examinations have been done to look at privacy concern with regards to social media sites, the objective of our investigation is to observationally assess the immediate and directing impact of privacy concern on users' acknowledgment of social media sites. Therefore, this study provides additional insights to the social media administrators for the dynamics of privacy issues social media settings. The significant impact of privacy concern on intention to use social media sites may explain why users keep using certain social media sites (for instance, Facebook) even

ISSN: 2394-7659
IMPACT FACTOR- 2.789

International Journal of Engineering Researches and Management Studies

after reports of privacy scams have been publicized. Based on the findings from this study, the administrators of social media sites should develop dynamic strategies and tactics to enhance users' acceptance level depending on their level of privacy concern. To connect users who have a relatively high level of privacy concern, efforts should be focused on improving the ease of usefulness of the site

.

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. *Arora, P., & Predmore, C. E. (2013). Social Media as a Strategic Tool: Going Beyond the Obvious. Advanced Series in Management , 11 (1), 115-127.*
4. *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.*
5. *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.*
6. *Bhandari, R. S., & Sharma, H. (2017). Impact of Social media on Brand Loyalty: Study of Buying Behaviour. International Journal of Applied Business and Economic Research , 15 (1), 297-308.*
7. *Boyd, D. M., & Ellison, N. B. (2008). Social networking sites:Defination, history and scholarship. Journal of Computer Mediated Communication , 13 (1), 210-230.*
8. *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.*
9. *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.*
10. *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.*
11. *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.*
12. *Cranor, L. ,. (2003). P3P: making privacy policies more useful. IEEE Security & Privacy , 1 (6), 50-55.*
13. *Culnan, M., & Armstrong, P. (1999). Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation. Organization Science , 10 (1), 104-115.*
14. *Diephay. (2016). Statistics and Market Data on Social Media & User-Generated Content. Germany: Statista.*
15. *Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. Information Systems Research , 17 (1), 61-80.*
16. *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.*
17. *Gudura, P., Cranor, L., & Arjula, M. (2006). User interfaces for privacy agents. ACM Transactions on Computer-Human Interaction , 13 (2), 135-178.*
18. *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.*
19. *Hong, W., & Thong, J. (2013). Internet privacy concerns: an integrated conceptualization and four empirical studies. Management Information Systems Quarterly , 37 (1), 275-298.*
20. *Hope, A. (2007). Risk taking, boundary performance and intentional school internet misuse. Discourse: Studies in the Cultural Politics of Education , 28 (1), 87-99.*
21. *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.*
22. *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.*

ISSN: 2394-7659
IMPACT FACTOR- 2.789

International Journal of Engineering Researches and Management Studies

23. *Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks:why we disclose. Journal of Information Technology , 25 (6), 109-125.*
24. *Li, K., Wang, X., Li, K., & Che, J. (2016). Information privacy disclosure on social network sites . Nankai Business Review International , 7 (3), 282-300.*
25. *Nissenbaum, H. (2004). Privacy as contextual integrity. Washington Law Review , 79 (1), 101-139.*
26. *Rosen, J. (2001). Out of context: the purposes of privacy. Social Research , 68 (1), 209-220.*
27. *Rotenberg, M., & Scott, J. (2015). Privacy in the Modern Age : The Search for Solutions. New York: The New Press.*
28. *Sheehan, K. (2002). Toward a typology or internet users and online privacy concerns. Information Society , 18 (1), 21-32.*
29. *Solove, D. (2001). Privacy and power: computer databases and metaphors for information privacy. Stanford Law Review , 53 (6), 1393-1462.*
30. *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.*
31. *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.*