EasyChair Preprint

№ 3053

Reality Check in Virtual Space for Privacy Behavior of Indian Users of Social Networking Sites

Sandeep Mittal and Priyanka Sharma

March 26, 2020

Reality Check in Virtual Space for Privacy Behavior of Indian Users of Social Networking Sites

Sandeep Mittal[1][0000-0001-7156-7045] and Priyanka Sharma[2][0000-0003-2651-7641]

[1]Cyber Security & Privacy Researcher, Former Director, NICFS (MHA), New Delhi, India
[2] Professor & Head, I.T. & Telecommunication, Raksha Shakti University, Ahmadabad, India
sandeep.mittal@nic.in

Abstract. The users of social networking sites intentionally or unintentionally reveal large amount of personal information about themselves. These SNSs' users have certain clues about the attitude of the persons with whom they interact in the physical world which are missing during online interaction. Therefore, their attitude in maintaining privacy of personal information in virtual space need to be understood. The present study is a maiden attempt to understand privacy attitude of the SNSs' users in online environment. The present study has identified and validated significant trends in privacy attitudes of Indian users of social networking sites and would serve as a starting point for future research.

Keywords: Information Privacy, Data Privacy Attitude, Data Privacy Law.

1 Introduction

The personal information thus shared in physical world has a limited and slow flow to others and generally dissipates with time with no trace after a relatively reasonable time span. Its impact on a person's reputation is also relatively limited to a close social- circle. The rise of the Internet, Web 2.0 and easy availability of smart devices has resulted in an era of privacy development where the use of social networking sites (SNSs) like Face book, LinkedIn, and Twitter etc. for exchanging information in virtual space has become the norm. The personal information exchanged over such SNSs generically differ from that in real world in that the persons exchanging information are not face to face with each other thus compromising the real world controls on the information, travels fast and far beyond the control of anyone and has perpetual availability on internet. The general privacy, initially defined either by value-based approach or cognate-based approach, gradually shifted in present information era to 'privacy as a right' concept to "control physical space and information". [1] The protection of privacy and confidentiality of this personal data at residence and in motion within and across the borders is a cause of concern.

In India, until the recent judgment by the 'Nine Judges Constitutional Bench' of Hon'ble Supreme Court of India [2], the right to privacy was not even recognized as a fundamental right and a data privacy legal framework is still lacking. This judgment

has recognized right to privacy as a fundamental constitutional right in India and has directed Government of India to put in place, a robust data privacy regime expeditiously for which Government of India has constituted a Committee called 'Justice B. N. Srikrishna Committee'. [3][3][3][3][3]As the current process of drafting a data privacy framework in India has commenced, the present study is scoped to understand the privacy attitudes of the Indian users of the SNSs.

2. The Literature Review

2.1 The Definition of Privacy

A perusal of the scholarly reviews on privacy reveals mainly two approaches to defining the general privacy, viz., value-based and cognate-based, the former being more prevalent in legal, sociological and political studies while the latter being more explored in psychological studies. In the present study a mix of these two approaches is used to explore the cognitive aspect (attitudes towards privacy) and the right-based aspect (expectations from law to protect privacy). As cognate-state approach, the general privacy is defined as "a state of limited access to a person" which narrowed down to Information systems broadly translates to "a state of limited access to information". [3] As cognate-control approach the general privacy is defined as "the selective control of access to the self" [4] and as "control of transactions between person(s) and other(s), the ultimate aim of which is to enhance autonomy or/and to minimize vulnerability" [5]. As a right-based approach, the general privacy is treated differently in different parts of the world, e.g., in the EU, privacy is seen as a fundamental human right; while in the U.S., privacy is seen as a commodity subject to the market and is cast in economic terms.

2.2 The Privacy and the Social Network(ing) Sites

In course of social interactions in the physical world, while an individual uses his physical senses to perceive and manage threats to his privacy, he has no such social and cultural cues to evaluate the target of self-disclosures in a visually anonymous online space of SNSs. Therefore, while the cognitive management of protection of privacy in offline world is performed unconsciously and effortlessly, deliberate actions are required for effective self-protection are required on SNSs.[6] These deliberative actions can be understood in terms of the "Theory of Planned Behavior" (TPB)[7]which stipulates that "an individual's intention is a key factor in predicting his or her behavior.

2.3 Understanding the Attitudes towards Privacy on SNSs

Several theoretical and empirical studies across disciplines have been conducted to understand the attitudes on privacy and data privacy protection laws in jurisdictions worldwide. A few findings relevant to the present work are enumerated here,

(a) An information disclosure by SNSs' users is associated with their level of concern for privacy. [8]
(b) SNSs' users are aware of privacy setting and change default settings as per their need. [9],[10]

(c) Perception of trust by SNSs' users improves with greater information disclosure by SNSs.[11]
(d) Privacy Policies of SNSs help in protecting privacy of SNSs' users. [12]
(e) Disclosure of personal information on SNSs is a bargaining process where perceived benefits and gratifications of networking outweigh the privacy. [13]
(f) More knowledge and experience of using the Internet improves privacy concern of SNSs' users. [14]
(g) Demographic factors influence SNSs' user's privacy behavior. [15]

In India, scholars have explored the attitude of Indian users of social networking sites with regard to trends in privacy behavior and thought process on need for a data privacy law in India.[15], [16], [17]

3. The Research Methodology

The population for the present study is the users of the SNSs in India grouped into five strata, namely, Law Enforcement Officers, Judicial and Legal Professionals, Academicians, Information Assurance and Privacy Experts and the Internet Users (other than listed in strata above) in India adopting disproportionate, stratified, purposive, convenience mixed sampling technique, and a statistically adequate sample size of 385 having 95% Confidence Level, 5% Margin of Error (Confidence Interval), 0.5 Standard Deviation and 1.96 Z-score was calculated.

A questionnaire was designed for this study by incorporating modified questions based on the Eurobarometer [16] and modified in Indian context and limited to the objectives of the present study. The variables included in the tool can be categorized as nominal and ordinal variables. A pilot study was conducted and reliability of instrument was checked by running reliability analysis which returned a Cronbach Alpha value of 0.700 and modified to adjust the scale and a Cronbach Alpha value of 0.795 was obtained which is well within the acceptable norms (< 0.700). [17] All the 401 respondents gave their informed explicit consent signifying their willing participation in this study. The data was collected during the month of August, 2017. The data was analyzed in SPSS for statistically significant trends regarding high privacy concern and its association for thought process on the expectations from law between variables by applying Pearson's Chi-Square (χ^2) Test of Independence with significance levels of 1% or 5% ($p < 0.01$ or $p < 0.05$) to test Null Hypotheses. The post-hoc analysis was done to determine the strength of the effect size of the association by calculating the Cramer's V values (ϕ').

As the study relied upon disproportionate, stratified, purposive, Convenience Sampling, the study may have limitation of non-generalization to wider population, and not taking into account the children presumptively below 18 years of age using the SNSs with fake accounts.

4 The Results, Data Analysis and Discussion

4.1 The Socio-Demographic Profile of Respondents

Out of 401 respondents, the majority was between 28 years to 45 year of age (42%), while the age group above 60 years has the minimum respondents (8.0%). Out of total population, 74.8% are males and 25.2% are females. The educational level of respondents were spread across categories with majority of the respondents being postgraduate (61%), followed by graduate (31%), Ph.D. (7%) and a small proportion (1%) below graduate level. The distribution of respondents across professional groups is multi-modal, i.e., Judiciary and Legal profession (10%), Law Enforcement (24%), Information Assurance and Privacy Experts (17%), Academic (20%) and other users of Internet (116, 28.9However, this ensures that all stakeholders involved in policy making for data privacy in India are accounted for. About 97% of respondents are users of SNSs (e.g., Face book, Twitter, LinkedIn, etc.). Majority of the respondents (46%) spent less than one hour on Internet followed by 29% of respondents spending between one to two hours on Internet. 83% of respondents have high level of online privacy literacy and 17% of respondents had low level of Online Privacy Literacy.

4.2 The Hypotheses Testing, Analysis and Discussion

As the major objective of the study is to understand the privacy attitudes of Indian users of social networking sites, we would test the following hypotheses,

4.2.1 Null-Hypothesis 1($H_0$1): There is no difference in degree of information disclosures by SNS users having high concern for privacy as compared with those having low concern for privacy.

4.2.1.1 Sub-hypothesis 1.1: Perceived reasons for information disclosure are significantly independent of the perceived sufficiency of the information given by SNSs regarding consequences of information disclosure

The Chi-square statistic and post-hoc analysis by calculating Cramer's V values (Table 1) and interpretation of the same indicates that the perceived disclosure by SNSs about consequences of information disclosure is found to be statistically significantly associated with:

a) the perceived reason 'access denied' for disclosure of information by users of SNSs at 5 per cent level of significance;
b) the perceived reason 'norm in modern lifestyle' for disclosure of information by users of SNSs at 1 per cent level of significance.

The association is not only significant but has a large effect size. However, the perceived reasons 'availing free services' and 'to connect with others' for disclosure of information by users of SNSs have no statistically significant association with the perceived disclosure by SNSs about consequences of information disclosure.

Table 1: Chi- square statistics for Sub-hypothesis 1.1

Sub- hypothesis 1.1 Perceived reasons for information disclosure are significantly independent of the perceived sufficiency of the information given by SNSs regarding consequences of information disclosure						
S. No.	**Null Hypotheses (H0)**	**$\chi 2$**	**df**	**p**	**Remarks**	**Effect Size (ϕ')**
1.1.1	The perceived reason 'access denied' for disclosure of information by users of SNSs is significantly independent of perceived disclosure by SNSs about consequences of information disclosure.	10.086	4	0.039	Significant ($P < 0.05$)	Large 0.20 (r= 4)
1.1.2	The perceived reason 'norm in modern lifestyle' for disclosure of information by users of SNSs is significantly independent of perceived disclosure by SNSs about consequences of information disclosure.	32.92	4	0.000	Significant ($p < 0.01$)	Large 0.80 (r= 4)
1.1.3	The perceived reason 'availing free services' for disclosure of information by users of SNSs is significantly independent of perceived disclosure by SNSs about consequences of information disclosure.	7.97	4	0.09	Insignificant	0.416 (r= 4)
1.1.4	The perceived reason 'to connect with others' for disclosure of information by users of SNSs is significantly independent of perceived disclosure by SNSs about consequences of information disclosure.	7.29		0.121	Insignificant	0.249 (r= 4)

4.2.1.2 Sub- hypothesis 1.2: Perceived reasons for information disclosure are significantly independent of the perceived concern for behavior monitoring by SNSs

The Chi-square statistic and post-hoc analysis by calculating Cramer's V values (Table 2) and interpretation of the same indicates that the perceived concern for behavior monitoring has statistically significant association with,

a) the perceived reason 'availing free services' for disclosure of information by users of SNSs at 5 per cent level of significance;
b) the perceived reason 'to connect with others' for disclosure of information by users of SNSs at 1 per cent level of significance.

The association is not only significant but has a large effect size. However, the perceived reasons *'access denied'* and *'norm in modern lifestyle'* for disclosure of information by users of SNSs have no statistically significant association with the perceived concern for behavior monitoring.

As these two factors viz., perception about disclosure by SNSs about consequences of information disclosure and concern about behavior monitoring by SNSs are indicative of level of concern for privacy, it is reasonable to conclude that there is significant difference in degree of information disclosures by SNS users having high concern for privacy as compared with those having low concern for privacy.

Therefore, in view of the foregoing discussion, the null hypothesis 1 (**$H_0$1**), that is, 'there is no significant difference in degree of information disclosures by SNS users having high concern for privacy as compared with those having low concern for privacy' is rejected and it is concluded that there is statistically significant difference

in degree of information disclosures by SNS users having high concern for privacy as compared with those having low concern for privacy and the effect size of this association is large.

Table 2: Chi square statistic for Hypothesis 1.2

Hypothesis 1.2 Perceived reasons for information disclosure are significantly independent of the perceived concern for behaviour monitoring by SNSs						
S. No.	**Null Hypotheses (H0)**	**$\chi 2$**	**df**	**p**	**Remarks**	**Effect Size (ϕ')**
1.2.1	The perceived reason 'access denied' for disclosure of information by users of SNSs is significantly independent of perceived concern for behaviour monitoring.	7.5	4	0.111	Insignificant	0.174 (r= 4)
1.2.2	The perceived reason 'norm in modern lifestyle' for disclosure of information by users of SNSs is not significantly dependent on perceived concern for behaviour monitoring.	3.338	4	0.503	Insignificant	0.261 (r= 4)
1.2.3	The perceived reason 'availing free services' for disclosure of information by users of SNSs is not significantly dependent on perceived concern for behaviour monitoring.	10.361	4	0.036	Significant ($p < 0.05$)	Large 0.475 (r= 4)
1.2.4	The perceived reason 'to connect with others' for disclosure of information by users of SNSs is significantly independent on perceived concern for behaviour monitoring.	14.52	4	0.006	Significant ($p < 0.01$)	Large 0.351 (r= 4)

4.2.2 Null- Hypothesis 2 ($H_0$2): Changing the Default Privacy Settings by the SNSs' Users is not associated with their understanding of the Privacy Policy

This hypothesis takes into account the understanding of privacy policy by the SNSs user and the ease with which they can change the default privacy settings.

Table 3: Chi- square statistic for Hypothesis 2

Null- Hypothesis 2 (H02): Changing the Default Privacy Settings by SNSs' Users is significantly not associated with their understanding of Privacy Policy						
S. No.	**Null Hypotheses (H0)**	**$\chi 2$**	**df**	**p**	**Remarks**	**Effect Size (?')**
2.1	The change of default privacy settings by SNSs' users is significantly independent of their understanding of the privacy policy.	10.76	4	0.029	Significant ($p < 0.05$)	Medium 0.4 (r= 5)
2.2	The ease of change in default privacy settings is significantly independent of SNSs' Users' understanding of the privacy policy.	12.44	4	0.014	Significant ($p < 0.05$)	Medium 0.4 (r= 5)

The Chi-square statistic and post-hoc analysis by calculating Cramer's V values (Table 3) and interpretation of the same indicates that, the change of default privacy settings by SNSs' users is significantly associated with their understanding of the privacy policy at 5 per cent level of significance. The ease of change in default privacy

settings is significantly associated with of SNSs' Users' understanding of the privacy policy at 5 per cent level of significance.

The association is not only significant but also has a medium effect size. Therefore, in view of the foregoing discussion, the null hypothesis 2 (**$H_0$2**), that is, 'changing the default privacy settings by SNSs' users is significantly not associated with their understanding of Privacy Policy' is rejected and it is concluded that changing the default privacy settings by SNSs' users is statistically significantly associated with their understanding of Privacy Policy and the effect size of this association is medium.

4.2.3 Null- Hypothesis 3($H_0$3): Privacy Policies of SNS help in protecting privacy of Social network users

This hypothesis factors into account the handling of privacy policy by the SNSs user, e.g., reading and understanding privacy policy, time spent on SNSs by user, reasons for ignoring the privacy policy and the resultant change in privacy behavior of SNSs users.

The Chi-square statistic and post-hoc analysis by calculating Cramer's V values (Table 4) and interpretation of the same indicates that,

a) The perceived change in resultant privacy behaviour of SNSs user is statistically significantly associated with,
b) The reading and understanding the privacy policy at 1 per cent level of significance with large size effect;
c) The handling of privacy policy by users at 1 per cent level of significance with large size effect.
d) The perceived reasons for ignoring the privacy policy are statistically significantly associated with,
e) Reading and understanding the privacy policy at 1 per cent level of significance with medium size effect,
f) Time spend daily by the user on SNSs at 5 per cent level of significance with medium size effect,
g) Handling of privacy policy by SNSs Users at 1 per cent level of significance with large size effect.

However, the study reveals that the time spent daily by the user on SNSs have no significant contribution to the resultant change in privacy behavior of the user.

Therefore, in view of the foregoing discussion, the null hypothesis 3 (**$H_0$3**), that is, privacy policies of SNSs do not help in protecting privacy of SNSs users is rejected and it is reasonable to conclude that privacy policies of SNSs help significantly in protecting privacy of SNSs users.

4.2.4 Null Hypothesis- 4 ($H_0$4): Privacy protection Behavior of SNSs' Users is different in Physical and Online Environments

The Chi-square statistic and post-hoc analysis by calculating Cramer's V values (Table 5) and interpretation of the same indicates that there is a statistically significant association between the behavior of SNSs user in physical and online environments at 1 percent level of significance with a small size effect. Therefore, the null hypothesis 4, that is, privacy protection behavior of SNSs' users is different in physical and on-

line environments is rejected and it is reasonable to conclude that there is statistically significant association of privacy protection behavior of SNSs' users in physical and online environments.

Table 4: Chi- square statistic for Hypothesis 3

Null- Hypothesis 3 (H03): Privacy Policies of SNS do not help in protecting privacy of SNSs Users						
S. No.	**Null Hypotheses (H0)**	**$\chi 2$**	**df**	**p**	**Remarks**	**Effect Size ?'**
3.1	The perceived resultant behavioural change is independent of reading and understanding privacy policy.	35.26	4	0.000	Significant ($p < 0.01$)	Medium 0.6 (r= 5)
3.2	The perceived resultant behavioural change on reading privacy policy is independent of time spend daily by the user on SNSs.	10.44	12	0.578	Insignificant	0.16 (r= 2)
3.3	The perceived resultant behavioural change after reading privacy policy is independent of handling the privacy policy by users.	75.43	12	0.000	Significant ($p < 0.01$)	Large 0.9 (r= 5)
3.4	The perceived reasons for Ignoring the Privacy Policy are independent of reading and understanding the privacy policy.	18.95	4	0.001	Significant ($p < 0.01$)	Medium 0.5 (r= 5)
3.5	The perceived reasons for Ignoring the Privacy Policy are independent of time spend daily by the user on SNSs.	22.93	12	0.028	Significant ($p < 0.05$)	Medium 0.5 (r= 5)
3.6	The perceived reasons for Ignoring the Privacy Policy are independent of handling of Privacy Policy by Users.	67.56	12	0.000	Significant ($p < 0.01$)	Large 0.9 (r=5)

Table 5: Chi- square statistic for hypothesis 4

NULL- Hypothesis- 4.0 : Privacy protection Behaviour of SNSs' Users is significantly different in Physical and Online Environments						
S. No.	**Null Hypotheses (H0)**	**$\chi 2$**	**df**	**p**	**Remarks**	**Effect Size (?')**
4.0	SNSs' Users, to protect their privacy, act differently in physical and online environments.	47.19	25	0.005	Significant ($P < 0.01$)	Small 0.20 (r= 6)

Table 6: Chi- square statistic for Hypothesis 5

Null- Hypothesis- 5 (H05) : Demographic Factors do not Influence SNSs' Users' Privacy Behaviour						
S. No.	**Null Hypotheses (H0)**	**$\chi 2$**	**df**	**p**	**Remarks**	**Effect Size (? ')**
5.1.1	Management of privacy default settings is not dependent on gender.	17.89	8	0.022	Significant ($P < 0.05$) Null is rejected.	Medium 0.3 (r= 5)
5.1.2	Handling of privacy policy is not influenced by gender.	7.13	6	0.309	Insignificant.	0.094 (r=2)
5.1.3	Resultant behaviour change after reading privacy policy is not dependent on gender.	4.78	8	0.780	Insignificant.	0.077 (r=2)
5.2.1	Management of privacy default settings is not dependent on education level of users.	28.14	16	0.030	Significant ($P < 0.05$) Null is rejected.	Medium 0.3 (r= 5)
5.2.2	Handling of privacy policy is not influenced by education level of users.	25.11	12	0.014	Significant ($P < 0.05$) Null is rejected.	Medium 0.3 (r= 5)
5.2.3	Resultant behaviour change after reading privacy policy is not dependent on education level of users.	21.99	16	0.114	Insignificant.	0.117 (r=2)
5.3.1	Management of privacy default settings is not dependent on profession of users.	12.77	16	0.689	Insignificant.	0.089 (r=2)
5.3.2	Handling of privacy policy is not influenced by profession of users.	35.79	12	0.000	Significant ($P < 0.01$) Null is rejected.	Medium 0.3 (r= 5)
5.3.3	Resultant behaviour change after reading privacy policy is not dependent on profession of users.	30.39	16	0.016	Significant ($P < 0.05$) Null is rejected.	Medium 0.3 (r= 5)
5.4.1	Management of privacy default settings is not dependent on age of users.	55.20	16	0.000	Significant ($P < 0.01$) Null is rejected.	Medium 0.4 (r= 5)
5.4.2	Handling of privacy policy is not influenced by age of users.	19.89	12	0.072	Insignificant. Null is retained.	0.128 (r=2)
5.4.3	Resultant behaviour change after reading privacy policy is not dependent on age of users.	26.03	16	0.054	Insignificant. Null is retained.	0.127 (r=2)

4.2.5 Null- Hypothesis- 5 ($H_0$5): Demographic Factors do not Influence SNSs' Users' Privacy Behavior

The Chi-square statistic and post-hoc analysis by calculating Cramer's V values (Table 6) and interpretation of the same indicates that there is a statistically significant association between

a) gender of users and management of default privacy settings at 5 per cent level of significance with a medium size effect;
b) education level of users and handling the privacy policy and management of default privacy settings both at 5 per cent level of significance with a medium size effect;
c) profession of users and handling of privacy policy at 1 percent level of significance and resultant behavioural change after reading the privacy policy at 5 per cent level of significance, both with medium size effect;
d) age of users and management of default privacy settings at1 per cent level of significance with a medium size effect;

Therefore, in view of the foregoing discussion, the null hypothesis 5 (**$H_0$5**), that is, demographic factors do not influence SNSs' users' privacy behavior is rejected and it is reasonable to conclude that demographic factors exert statistically significant influence over SNSs users' privacy behavior.

5 Conclusions

To sum up, the Chi- square test and post hoc analysis of data has revealed significant associations regarding privacy attitudes of Indian users of SNSs as follows;

a) There is significant difference in degree of information disclosures by SNS users having high concern for privacy as compared with those having low concern for privacy.
b) Changing the default privacy settings by SNSs' users is statistically significantly associated with their understanding of Privacy Policy.
c) Privacy policies of SNSs help significantly in protecting privacy of SNSs users.
d) There is statistically significant association of privacy protection behavior of SNSs' users in physical and online environments.
e) Demographic factors exert statistically significant influence over SNSs users' privacy behavior.

References

[1] H. J. Smith, T. Dinev, and H. Xu, "Information privacy research: an interdisciplinary review," *MIS quarterly,* vol. 35, no. 4, pp. 989-1016, 2011. MIS quarterly

[2] "JUSTICE K S PUTTASWAMY v Union of India," ed: SUPREME COURT OF INDIA (Nine Judges Costitutional Bench), 2017.

[3] Government of India. (2017). *3(6)j2017-CLES Constitution of a Committee of Experts to deliberate on a data protection framework for India* [Online] Available: http://meity.gov.in/writereaddata/files/MeitY_constitution_Expert_Committee_31.07.2017.pdf

[4] I. Altman, "The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding," 1975.

[5] S. T. Margulis, "Conceptions of privacy: Current status and next steps," *Journal of Social Issues,* vol. 33, no. 3, pp. 5-21, 1977.

[6] M. Z. Yao, "Self-protection of online privacy: A behavioral approach," in *Privacy Online*: Springer, 2011, pp. 111-125. Privacy Online.

[7] I. Ajzen and M. Fishbein, "The influence of attitudes on behavior," *The handbook of attitudes,* vol. 173, no. 221, p. 31, 2005.

[8] R. Gross and A. Acquisti, "Information revelation and privacy in online social networks," in *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*, 2005: ACM, pp. 71-80.

[9] K. Strater and H. Richter, "Examining privacy and disclosure in a social networking community," in *Proceedings of the 3rd symposium on Usable privacy and security*, 2007: ACM, pp. 157-158.

[10] C. Dwyer, S. Hiltz, and K. Passerini, "Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace," *AMCIS 2007 proceedings,* p. 339, 2007. AMCIS 2007 proceedings

[11] B. Debatin, J. P. Lovejoy, A.-K. Horn, and B. N. Hughes, "Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences," *Journal of Computer-Mediated Communication,* vol. 15, pp. 83-108, 2009. Journal of Computer-Mediated Communication

[12] N. B. Ellison, J. Vitak, C. Steinfield, R. Gray, and C. Lampe, "Negotiating privacy concerns and social capital needs in a social media environment," in *Privacy online*: Springer, 2011, pp. 19-32. Privacy online.

[13] R. LaRose, D. Mastro, and M. S. Eastin, "Understanding Internet usage: A social-cognitive approach to uses and gratifications," *Social science computer review,* vol. 19, no. 4, pp. 395-413, 2001. Social science computer review

[14] Z. Tufekci, "Grooming, gossip, Facebook and MySpace: What can we learn about these sites from those who won't assimilate?," *Information, Communication & Society,* vol. 11, no. 4, pp. 544-564, 2008.

[15] S. MIttal and P. Sharma, "Indo-Privacy-Barometer v1.0 : Discerning Trends in the Privacy Attitude of Indian Users of Social Networking Sites," *International Journal of Computer Sciences and Engineering,* Survey Paper vol. 7, no. 5, pp. 306- 314, 2019.

[16] S. Mittal and P. Sharma, "A Study of the Privacy Attitudes of the Users of the Social Network(ing) Sites and Their Expectations from the Law in India," presented at the International Conference on Intelligent Systems Design and Applications ISDA 2017 : Intelligent Systems Design and Applications, New Delhi, 22 March 2018, 2018. [Online]. Available: https://link.springer.com/chapter/10.1007%2F978-3-319-76348-4_100.

[17] S. Mittal and P. Sharma, "Contouring the Behavioral Patterns of the Users of Social Network (ing) Sites and the Need for Data Privacy Law in India: An Application of SEM-PLS Technique," in *International Conference on Innovations in Bio-Inspired Computing and Applications*, 2018: Springer, pp. 440-451.

[18] S. Eurobarometer, "359. 2011," *Attitudes on Data Protection and Electronic Identity in the European Union,* 2011.

[19] I. Serbetar and I. Sedlar, "Assessing Reliability of a Multi-Dimensional Scale by Coefficient Alpha," *Revija za Elementarno Izobrazevanje,* vol. 9, no. 1/2, p. 189, 2016.