IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.-7, Issue-5, May 2019 E-ISSN: 2347-2693

Indo-Privacy-Barometerv 1.0: Discerning Trends in the Privacy Attitude of Indian Users of Social Networking Sites

Sandeep Mittal[1*], Priyanka Sharma[2]

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

Corresponding Author: sandeep.mittal@nic.in

DOI: https://doi.org/10.26438/ijcse/v7i5.306314 | Available online at: www.ijcseonline.org

Accepted: 10/May/2019, Published: 31/May/2019

Abstract. In an era of online social networking, the data privacy is becoming on important topic for researchers to explore. To regulate collection, use and processing of personal data, one needs to understand the behavioral attitude of users of internet so that their need for a law can be assessed. Several studies in this regard have been conducted in other parts of the world where data privacy law is in place, but in India the data privacy was not even a right till recently, when Supreme Court of India declared data privacy as part of the fundamental right of privacy in accordance with constitution of India. The present study is a maiden attempt in India to understand the privacy attitude of the Indian users of social networking sites.

***Keywords*:** Indobarometer, Data Privacy, Privacy Attitudes, Social Networking Sites, SNSs, Human behavior in Cyber Space.

I. INTRODUCTION

The general privacy beliefs are results of complex interaction of social norms and moral value beliefsoften mediated in space and time by a number of social variables at individual and collective levels[1].In real-life social interactions, the individuals have a control over the personal information shared amongst each other. 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 timespan. Its impact on a person's reputation is also relatively limited to a relatively 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 network(in) sites (SNSs) like Facebook, LinkedIn, Twitter etc. for exchanging information in virtual space has become the norm [2]. The user generated content, mostly beyond the knowledge and comprehension of SNSs' users, and algorithms of the web aggregating services further worsens the privacy scenario today with SNSs sensing the every breath and the every step one takes in real life. 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-disclosure 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 is required on SNSs [3-6]. The scope of the present study is to analyze the trends in privacy behaviour of the Indian users of social networking sites.

II. THE LITERATURE REVIEW

Although the present study is maiden attempt in India to understand the privacy attitude of the users of social networking sites, 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 important findings relevant to the present work are enumerated below:

1. Information disclosures by users of SNSs are associated with their levels of concern for privacy[7].
2. Users of SNSs are aware of privacy settings and change default settings as per their needs [7].
3. The privacy policies of SNSs help in protecting the privacy of users of SNSs' [8].
4. Disclosure of personal information on SNSs is a bargaining process wherein the perceived benefits and gratifications of networking outweigh the privacy [8].
5. Demographic factors influence the privacy behavior of users of SNSs [9, 10].

III. 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 and modified in Indian context and limited to the objectives of the present study[11]. The variables included in the tool can be categorized as nominal and ordinal variables. All the 401 respondents gave their informed explicit consent signifying their willing participation in this study.The trends were analyzed using Microsoft Excel Software.

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.

IV. RESULTS

The 'psychological constructs' are generally considered latent as they do not measure a factor directly but do so only through indirect theoretical inference, and "the term 'measurement' in psychology is rather to be interpreted as an extended form of observation [12]."Detailed reviews on measuring attitudes are made by scholars [13]. The data in the present study is nominal and ordinal, and described as categorical [14].Based on the literature review [15, 16], the present study, for the purpose of descriptive analyses, would treat the variables as observations rather than nominal and ordinal variables in the strict sense, thus avoiding the use of descriptive statistics like mean, median, or standard deviation, as these would not be appropriate for describing the true attitudes measured (read observed) using the categorical data [17].

4.1 The Socio-demographic Profile of Respondents

The socio-demographic profile comprising the gender, age, profession, educational levels, and the time spent on discussion on the Internet is significant, as it has the potential of influencing the attitudes of the respondents, and is discussed in detail below.

(a) A majority of the 401 respondents were in the age group of 28 to 45 years (42 per cent), while the minimum respondents were those belonging to the age group above 60 years (8.0 per cent). This probably reflects the low level of need for networking among the respondents above the age of 60 years, which is also the general age for retirement from jobs in India. Simultaneously, the finding reflected a high level of need for professional and social networking for people between the ages of 28 and to 45 years, the age group during which the respondents would generally aspire to broaden their professional and social contacts. There are approximately an equal number of respondents in the categories above (24 per cent) and below (26 per cent) the modal category (**Fig.1**).

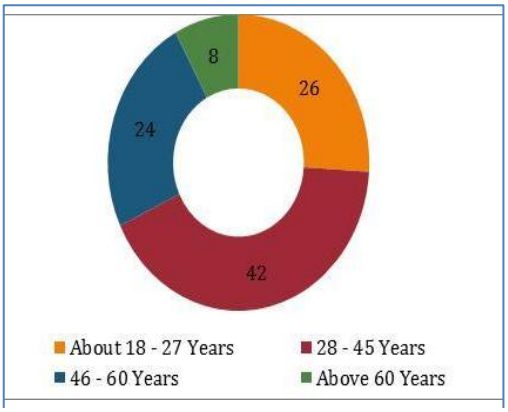

Fig.1. Relative frequency distribution of age of the respondents

(b) Among the total sample population,74.8 per cent are males and 25.2 per cent are females (**Fig.2**). This is in consonance with the Internet usage statistics for 2016 in India, that is, among the daily users of the Internet, 40 per cent are females located in urban areas while 25 per cent are females based in rural areas.

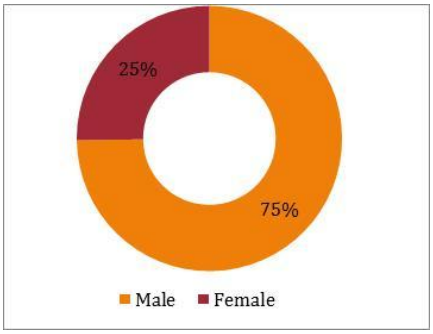

Fig.2. Relative frequency distribution of gender of respondents

The educational levels of the respondents were spread across diverse categories, with a majority of the respondents being post-graduates (61 per cent), followed by graduates (31 per cent), and Ph.Ds (7 per cent), and a small proportion (1 per cent) having education below the graduate level (**Fig.3**).

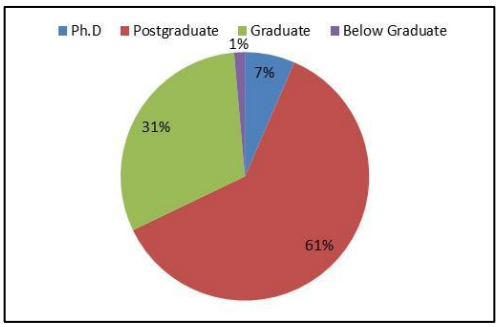

Fig.3. Relative frequency distribution of educational level of respondents

A cross-tabulation with gender reveals that only 56.3 per cent of the females, as compared to 63.0 per cent of the males, were post-graduates. The relative frequency distribution of females versus males was comparable among the other categories, that is, graduates (F: M: 34: 30) and Ph.Ds (F: M: 7:6) (**Fig.4**).

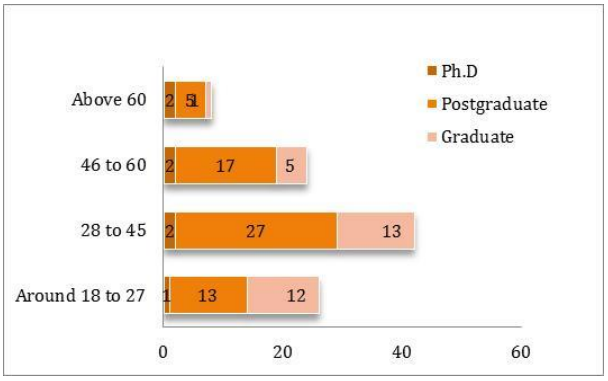

Fig.4. Educational level spread over age groups

(c) The distribution of respondents across professional groups, which is multi-modal, is as follows: that is, Judiciary and the Legal Profession (10 per cent), Law Enforcement (24 per cent), Information Assurance and Privacy Experts (17 per cent), Academic (20 per cent), and other users of the Internet (116, 28.9 per cent). This is due to the 'disproportionate- stratified' and purposive sampling technique adopted for convenience. However, this ensures that all the stakeholders involved in policymaking for data privacy in India are accounted for (
Fig.5).

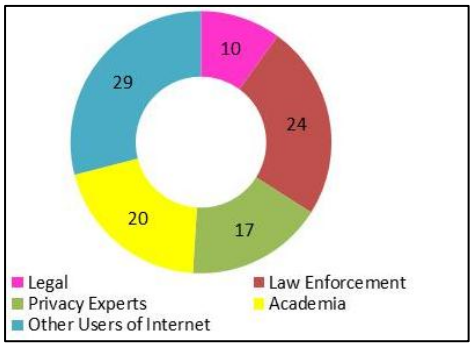

Fig.5. Relative frequencies of the professions of respondents

(d) About 97 per cent of the respondents are the users of SNSs (including Facebook, Twitter, and LinkedIn, among other sites). A majority of the respondents (46 per cent) spent less than one hour on the Internet, followed by 29 per cent of the respondents who spent one to two hours on the Internet. These results could be explained by the fact that these respondents are highly qualified and gainfully employed in high positions in their respective professions, which leaves them with little to spend on the Internet (**Fig.6**). About 45 per cent of the male and 47 per cent of the female respondents spent less than one hour per day on the Internet. Only 24 per cent of the females, as compared to 31 per cent of the males spent one to two hours per day on the Internet. However, 16 per cent of the females, as compared to 10 per cent of the males spent more than three hours per day on the Internet.

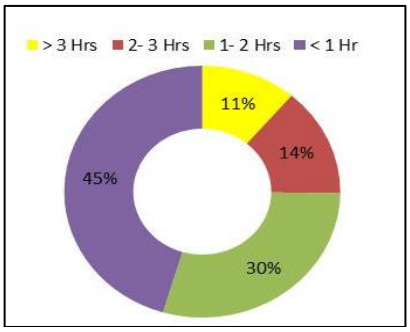

Fig.6. Cumulative time spent by the respondents on the Internet

1.2 Online Privacy Literacy Assessment

The respondents were asked a set of exploratory questionsto assess their "Online Privacy Literacy Levels', which were to be answered on a 'True' or 'False' scale. The questions were designed to encompass five dimensions of Online Privacy Literacy. The responses to these questions were summated and the Online Privacy Literacy percentage was calculated, which revealed that 83 per cent of the respondents had a high level of online privacy literacy while 17 per cent had a low level of online privacy literacy. This distribution achieves the aim of purposive sampling by ensuring that the responses to the questionnaire are considered the opinion of the population that is largely literate in terms of online privacy issues (**Fig.7**).

However, the proportion of the females having knowledge about the laws and legal aspects (87 per cent) was marginally lower than that of the males (92 per cent). Similarly, the proportion of females having knowledge about personal strategies for data protection (for example, the use of a single password for multiple accounts was lower (56 per cent) than that of males (64 per cent).

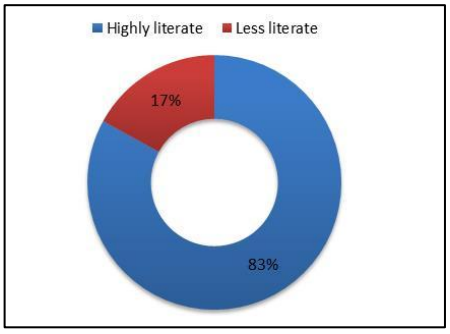

Fig.7. Online privacy literacy levels of the respondents

4.3 The Attitudes: A Descriptive Analysis

This study explores the attitudes of Indian users of SNSs, and the responses to the variables have been grouped into various constructs to describe and understand the attitudes of the population. These constructs are categorized [9]as Disclosure of Personal Information, Attitude towards Disclosure of Personal Information, Identity Protection, Users' Awareness about Access of Data by Third Parties, Perceived Control over Personal Data, Expectations from SNSs holding Personal Data, Respondents' Access to their Personal Data held by SNSs, and Thought Process on the Regulation of Personal Data in India. Each of these constructs has been discussed in the following sub-sections.

Attitude toward Disclosure of Personal Information.

The disclosure of personal information by the users on SNSs is the *raison d'être* for the functioning of SNSs. The disclosure may be intentional or unintentional, obvious or hidden, voluntary or forced, or a mix of all these most of the time. The respondents were asked to identify the three most important pieces of information they consider to be personal (**Fig.8**). Financial Information (59 per cent), Aadhaar details, Passport, Licence (56 per cent), and Biometrics (46 per cent) were among the three most important pieces of information identified as personal by the respondents. Surprisingly, Friends' List (4 per cent), Work History (5 per cent), and Medical Information (12 per cent) were not considered as important personal information by a majority of the respondents. This aspect is worrisome as the respondents demonstrate a low level of concern particularly regarding the information pertaining to friends, thereby exposing the latter's privacy to risk.

Among the 183 respondents who considered Biometrics as the most important personal information, 79 per cent were males and 20.8 per cent were females, and a majority of them were post-graduates (61.7 per cent) in the age group of 28 to 45 years (44.8 per cent). Among the 226 respondents who considered Aadhaar, Passport, and Licence as their most important pieces of personal information, 77.9 per cent were males and 22.1 per cent were females, and again a majority of them were post-graduates (61.5 per cent), belonging to the age group of 28 to 45 years (46 per cent).

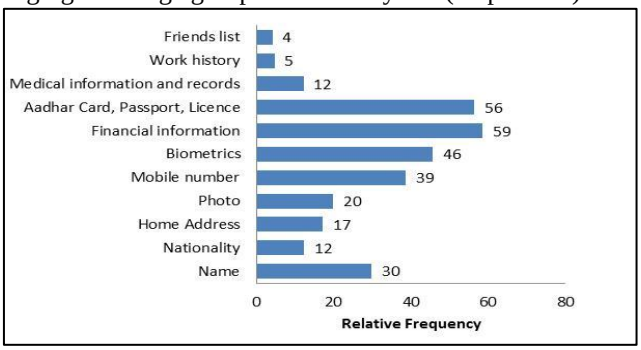

Fig.8. Personal information considered mostimportant by the respondents

While the gender-wise spread of the sample population for the three most important pieces of personal information is broadly in consonance with the proportion of the gender of the population, the age-wise spread is fitted in favour of the age group of 28 to 45 years. This may be due to the exposure of the respondents in this age group to Information Communication Technology (ICT) as part of their education and profession. Further, the Individual Usability Pillar (Index) [18] for India is very low (2.1) as compared to that of the UK (6.6) and USA (6.2) on a scale of 7, with the former placed at rank 121, and the latter two at ranks 5 and 17, respectively, among the 139 countries in the world.

Reasons for Disclosing Personal Information on SNSs.

On being asked about the reason for disclosing information on SNSs, a majority of the respondents (63 per cent) expressed the perception that the SNSs would deny them access to the site if they did not disclose their personal information, followed by 1 per cent of the respondents who disclosed their personal information to connect with others. A small proportion of the respondents disclosed their personal information to avail of free services (11 per cent) while 12 per cent of the respondents made the disclosure thinking that it is a norm in the present-day world (**Fig.9**).

Out of 249 respondents who reasoned that they would be denied access to the site if they did not disclose their personal information, a majority were post-graduates (63 per cent), and in the age group of 28 to 45 years (45 per cent). The gender-wise distribution of the respondents indicates that 78 per cent of them were males and 22 per cent were females.

The objective of connecting with others was the second most important reason for disclosing personal information on SNSs, and a majority of these respondents are post-graduates (58 per cent) in the age group of 28 to 45 years (84 per cent), while 69 per cent of them were males and 31 per cent were females. Among those who felt that disclosing information is a norm in modern-day lifestyle, 52 per cent were in the age group of 18 to 27 years, and 85 per cent were males. An interesting observation is that information and privacy experts were least willing to disclose information while trying to connect with others (13 per cent).

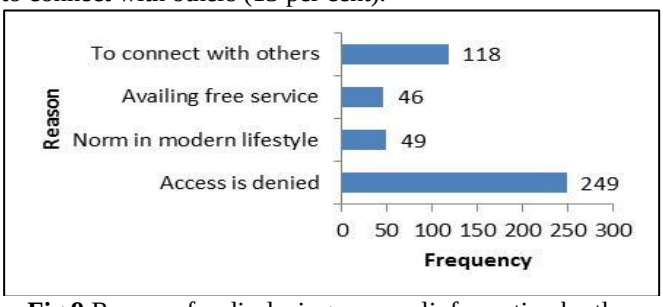

Fig.9. Reasons for disclosing personalinformation by the respondents

Among those who wanted to avail of free services of SNSs, 44 per cent were in the age group 28 to 45 years, followed by respondents in the age group of 18 to 27 years (26 per cent), and 76 per cent of them were males and 24 per cent were females.

Most Important Risks of Information Disclosure.
The three most important risks of information disclosure, as identified by a majority of the respondents are third party sharing their data without consent (86 per cent); identification of theft (75 per cent); and fraud (72 per cent). The targeted advertisement was rated as a risk only by 33 per cent of the respondents, followed by the risk to reputation (24 per cent), and professional discrimination (10 per cent). Probably targeted advertisements are not treated as risks by a majority of the respondents as they consider it as a fair trade for free services and as the usability index is low in India, the online risk to reputation is not so common as of now. An analysis of the data revealed that a proportion of the ratings given by the respondents is, in general, in consonance with the distribution of the respondents across gender, educational levels, and age groups (**Fig.10**).

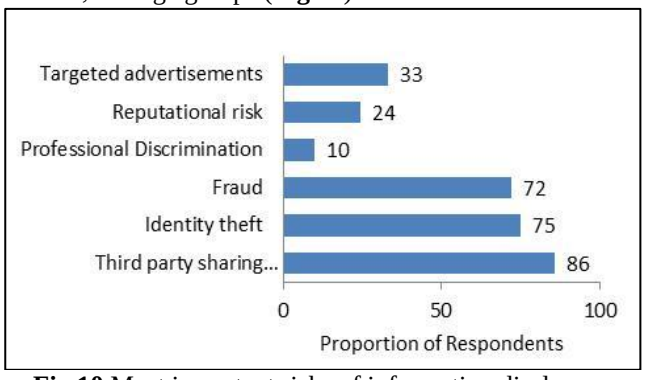

Fig.10. Most important risks of information disclosure

Concern about Monitoring and Recording Users' Behaviour by SNSs.
As regards the concern about behaviour monitoring, a majority of the respondents (87 per cent) were concerned about monitoring and recording of behaviour by the SNSs (in terms of browsing habits, navigation, and downloads, among other behavioural trends); while a small proportion of the respondents (13 per cent) were not concerned about behaviour monitoring (**Fig.11**). An interesting trend is that the respondents who spent relatively less time on the Internet (< 1 hour) were more concerned about the monitoring and recording of their behaviour (87 per cent) as compared to the respondents (29 per cent) who spent more time on the internet (2 to 3 hours). Perhaps while spending more time on online social networking, the users lower their guards and display a low level of concern regarding the monitoring of their behaviour.

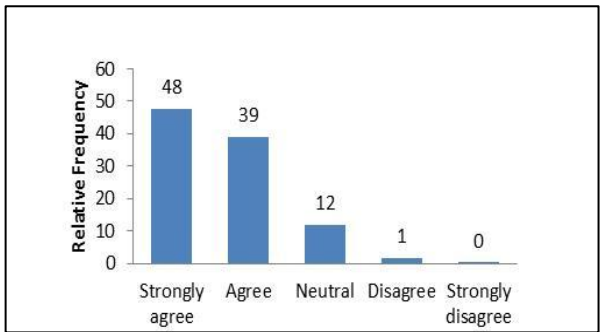

Fig.11. Respondent's concerns about behaviour monitoring

Attitudes towards Identity Protection.
The protection of users' identity to prevent misuse by others is an important consideration in day-to-day life while one is engaging in in real-life transactions with others. With the increased use of the Internet, such interactions have extended to SNSs, where interactions with other members take place either directly or indirectly. The following questions have been explored in this section: What actions are taken by respondents to protect their identities in real day-to-day life, and do they take similar actions while disclosing information on SNSs? Do the actions, so taken, correspond to or differ from each other?

Protection of Identity in Daily Life.
When asked about what they do to protect their identity in their daily life (not on SNSs), 68 per cent of the respondents said that they give the minimum required information while 52 per cent of the respondents said that they do not disclose financial information like payment card details, PIN, etc., while 35 per cent of the respondents admitted to adjusting the information depending upon the trust level. Only 11 per cent of the respondents were shredding old bills, invoices, and credit card receipts to protect their privacy in day-to-day life. Interestingly, only 2 per cent of the respondents were not taking any action to protect their identity.

Protection of Identity on SNSs.
In order to compare the attitude of users in daily life with their attitude on the SNSs, the respondents were asked about various acts on SNSs, corresponding to the respective acts pertaining to daily life. Interestingly, the relative frequencies of the acts for identity protection on SNSs, in general, correspond to acts in daily life (**Fig.12**). The only exception to the general match for acts in real life and virtual life is the act of non-disclosure of financial information. While 52 per cent of the respondents averred that they do not disclose financial information in their daily life, only 28 per cent of the respondents said that they change the security settings of their browsers to enhance privacy, implying that a significant number of respondents lowered their guards while using SNSs.

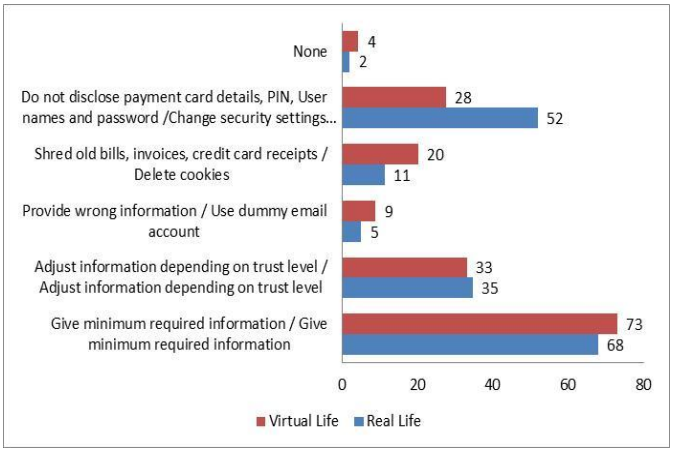

Fig.12. Acts of respondents to protect privacy in real versus virtual life

Awareness about access of personal data by Third Parties.
The privacy policies disclosed by the SNSs may play an important role in decision-making by users regarding the handling of their personal information. Therefore, understanding the attitudes of users in handling the privacy policies of SNSs would be useful for understanding their privacy concerns and behaviour. These aspects are explored in this section.

Handling the Privacy Policy.
All the SNSs have a privacy policy. When asked about how they handle the privacy policy of SNSs, 53 per cent of the respondents indicated that they read the privacy policy out of which only 18 per cent of the respondents understand the privacy policy. A majority of the respondents (38 per cent) do not read the privacy policy while 9 per cent of the respondents completely ignored the privacy policy, thus signifying low concern for privacy (**Fig.13**). Among the 78 per cent of the respondents who do not read or ignore the privacy policy were males while 22 per cent of them were females. A majority of the respondents who claimed to have read and understood the privacy policy were in the age group of 18 to 27 years (42 per cent), followed by those in the age group of 28 to 45 years (39 per cent). Among the respondents who do not read the privacy policy, a majority were post-graduates (60 per cent), belonging to the age group of 28 to 45 years (26 per cent). Among the professionals who reported not reading the privacy policy were those belonging to the judicial/legal (8 per cent), law enforcement (33 per cent), and information assurance (12 per cent) fraternity, members of academia (14 per cent), and Internet users (34 per cent).

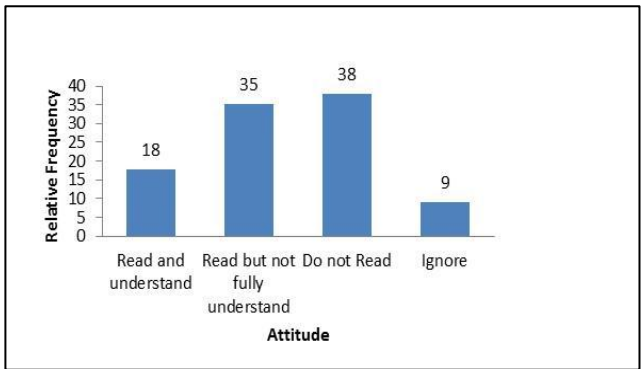

Fig.13. Attitudes toward reading of the privacy policy

Behaviour Change after Reading the Privacy Policy.
When asked if they adopted a change in their behaviour after reading the privacy policy. 47 per cent of the respondents answered in the affirmative while 53 per cent of the respondents stated that they failed to adopt any change in their behaviour after reading the privacy policy (**Fig.14**).

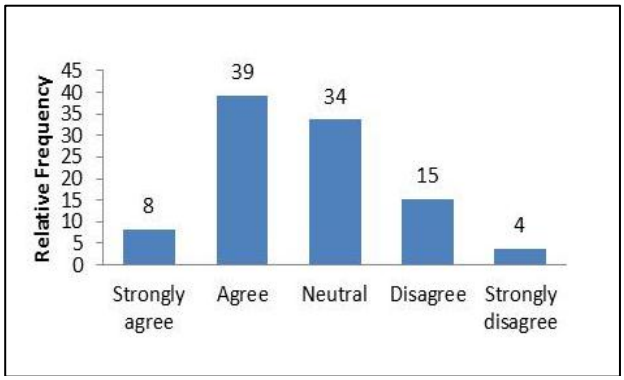

Fig.14. Adoption of change in behaviourafter reading the privacy policy

Reasons for Ignoring the Privacy Policy.
Among the reasons cited for ignoring the privacy policy, the inordinately lengthy text and use of complex language in the policy were the main reasons as to why the respondents ignored the privacy policy, which was cited by 59 per cent of the respondents while 17 per cent of the respondents believed that the SNSs would anyway not honour the privacy policy. Only 10 per cent of the respondents actually believed that the SNSs would adhere to the privacy policy while 7 per cent each either did not have the time to read the privacy policy or expected the law to protect them, signifying a low level of concern for privacy (**Fig.15**). Expecting only the law to protect them is akin to leaving one's BMW car on the road with the keys in the ignition, and without locking the door, believing that the police would ensure that it is not stolen, and such an attitude obviously indicates lack of due diligence.

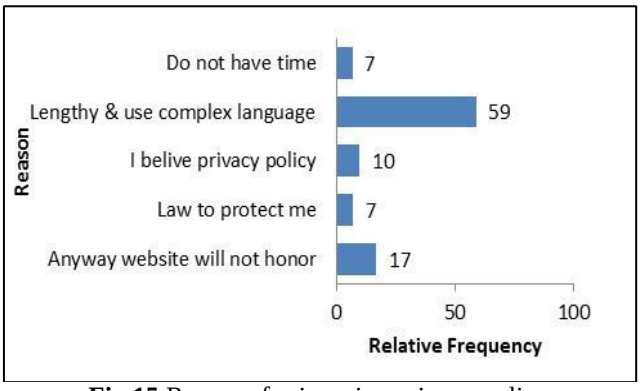

Fig.15. Reasons for ignoring privacy policy

Sufficiency of Information on Terms of Use Given by the SNSs.

The perceptions of the respondents, as to whether they were informed about the conditions of collection of the personal data, and its further uses at the time of becoming a user of SNS, were equally divided, with 50 per cent of the respondents perceiving that the SNSs provided sufficient information on the terms and uses of the personal information collected by them, while the other half believed the opposite (**Fig.16**).

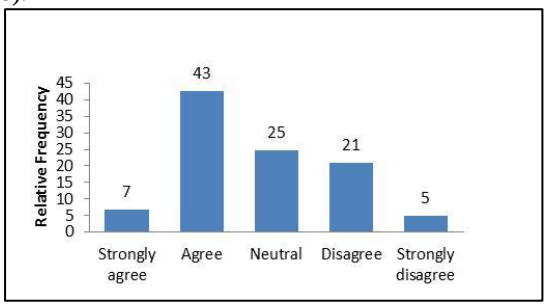

Fig.16. Sufficient information provided by the SNSs on terms of use

Perceived Control over information disclosed on the SNSs.

Once the personal information has already been disclosed by the users of SNSs, what are the users' perceptions regarding their control (for example, ability to change, delete) over such information. While 29 per cent of the respondents perceived that they had no control over the information they disclosed to SNSs, 18 per cent of the respondents believed that they had full control over the information they disclosed to the SNSs. However, a majority of the respondents (52 per cent) believed that they have only partial control over the information disclosed by them on the SNSs (**Fig.17**). Among the respondents believing that they had full control over the information disclosed, 66 per cent were males and 34 per cent were females; 45 per cent were in the age group of about 18 to 27 years, and 42 per cent were in the age group of 28 to 45 years. The respondents perceiving full control over the information disclosed by them is perhaps indicative of their ignorance or over-confidence, and also highlights their low level of concern for privacy protection.

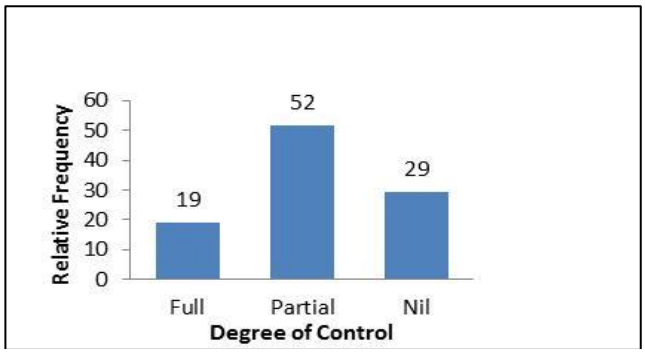

Fig.17. Control over disclosed information on the SNSs

Expectations from SNSs.

The SNSs collect the personal information of users including metadata without their consent through the use of technology for commercial advertisements.

(a) A majority of the respondents (55 per cent) did not feel comfortable with the SNSs collecting their personal data for commercial advertisements, but 28 per cent of the respondents were comfortable with the SNSs collecting their personal data for commercial advertisements, which again signifies the poor level of concern for privacy among this category of respondents (**Fig.18**).

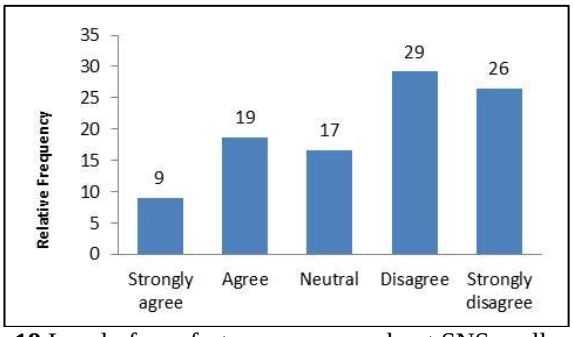

Fig.18. Level of comfort among users about SNSs collecting their personal data for commercial advertisements

(b) When asked if their approval or explicit consent is required for collection and processing of their personal data, a majority of the respondents (55 per cent) answered that their consent is always required, while 35 per cent of the respondents said that they wanted their approval or consent to be taken only for sensitive information. Only a small proportion of the respondents (10 per cent) did not want their approval or explicit consent to be taken for the collection of their personal data, signifying the low level of poor concern for their privacy among these respondents (**Fig.19**).

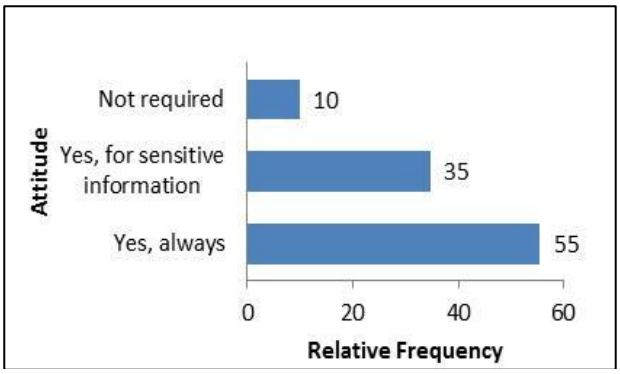

Fig.19. Perceptions regarding the need for explicit Consent by SNSs for processing of personal data

User's Access to their Personal Data held by the SNSs.
A personal profile on the SNSs contains vital information like name, age, gender, location, interests, and photograph of the user. The user can adjust the profile visibility by managing the privacy settings. This section explores the attitudes of the respondents with regard to managing of their default privacy settings (**Fig.20**).

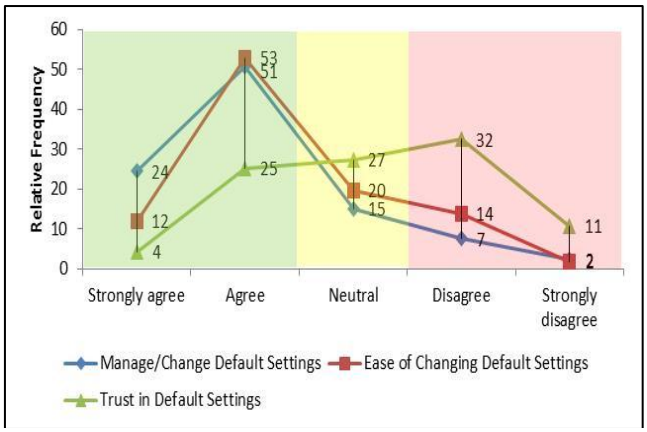

Fig.20. Attitudes toward the privacy settings of SNSs

(a) When asked whether they manage their profile visibility by changing the default privacy settings of the SNSs, a majority of the respondents (75 per cent) replied in the affirmative while 25 per cent of the respondents said that they did not manage their default privacy settings, thus signifying their low level of concern for privacy.

(b) Regarding the ease with which the default privacy settings can be changed, a majority of the respondents (55 per cent) felt that it is easy to change the default privacy settings while 16 per cent of the respondents felt that it was not easy to change the default privacy settings. A substantial proportion of the respondents (20 per cent) could not decide the level of ease with which the default privacy settings could be changed.

(c) As regards the issue of trust in the default privacy settings, a majority of the respondents (43 per cent) said that they did not trust the default privacy settings of the SNSs in protecting their data privacy but 37 per cent of the respondents said that they did trust the default privacy settings, with the latter thus showing low level of concern for privacy. A substantial number of the respondents (27 per cent) were undecided regarding the trust level of the default privacy settings.

V. CONCLUSIONS

The present study explores the attitudes of Indian users of SNS and the following descriptive trends on data privacy attitudes were discerned in the present study:

1. The three most important pieces of personal information identified are financial information, data in the Aadhaar, Passport, and License, and Biometrics. The friends' list, work history and medical information are not considered as important pieces of personal information.
2. The most important reason for information disclosure was the denial of access by the SNSs if the information is not disclosed, followed by an urge to connect with others.
3. The three most important risks of the disclosure of information disclosure identified are data sharing without consent, identity theft and the possibility of frauds.
4. The monitoring and recording of behavior is a major privacy concern.
5. The acts of users to protect their identity in daily life and on SNSs are, in general, similar except while doing financial transactions, users being less careful in online environment.
6. While a majority of the respondents read the privacy policy of the SNSs, only few understand the same. A majority of the respondents failed to adopt a change after reading the privacy policy. The lengthy and complex text was a major reason for the respondents ignoring the privacy policy.
7. A majority of the respondents perceived that they had only partial control over the information disclosed by them.
8. A majority of the respondents were not comfortable with the SNSs collecting their personal data for commercial advertisements.
9. A majority of the respondents wanted their explicit consent to be always taken.
10. A majority of the respondents did not trust the default settings.
11. While the majority of respondents perceived a part role for all the stakeholders including the Government, substantial population envisaged that it was the full responsibility of the Government to protect their information.

The present study is a maiden attempt to understand the behavior and attitude of the users of social networking sites in India. These trends would help policy makers understand the need for an appropriate law to regulate the data privacy in India. This would help them understand the areas of data privacy which cannot be regulated by correcting the human

attitude would need to be regulated by the laws mandating 'privacy by default' and 'privacy by design'. These general trends, however, would need to be validated by exploratory statistical analysis and structural equation modelling studies.

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] A. F. Westin, "Social and political dimensions of privacy," Journal of social issues, vol. 59, no. 2, pp. 431-453, 2003.

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

[4] I. Ajzen, "From intentions to actions: A theory of planned behavior," in Action control: Springer, 1985, pp. 11-39.

[5] I. Ajzen, "The theory of planned behavior," Organizational behavior and human decision processes, vol. 50, no. 2, pp. 179-211, 1991.

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

[7] 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, pp. 71-80: ACM.

[8] 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

[9] F. Stutzman and J. Kramer-Duffield, "Friends only: examining a privacy-enhancing behavior in facebook," in Proceedings of the SIGCHI conference on human factors in computing systems, 2010, pp. 1553-1562: ACM.

[10] 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.

[11] S. Eurobarometer, "359. 2011," Attitudes on Data Protection and Electronic Identity in the European Union, p. 42, 2011.

[12] D. Borsboom, Conceptual issues in psychological measurement. Universiteit van Amsterdam [Host], 2003.

[13] M. Lovelace and P. Brickman, "Best practices for measuring students' attitudes toward learning science," CBE-Life Sciences Education, vol. 12, no. 4, pp. 606-617, 2013.

[14] A. Agresti, "An introduction to categorical data analysis, 2nd edn. Hoboken," ed: NJ: Wiley-Interscience, 2007.

[15] S. Jamieson, "Likert scales: how to (ab) use them," Medical education, vol. 38, no. 12, pp. 1217-1218, 2004.

[16] H. J. Gardner and M. A. Martin, "Analyzing ordinal scales in studies of virtual environments: Likert or lump it!," Presence: Teleoperators and Virtual Environments, vol. 16, no. 4, pp. 439-446, 2007.

[17] H. M. Marcus-Roberts and F. S. Roberts, "Meaningless statistics," Journal of Educational Statistics, vol. 12, no. 4, pp. 383-394, 1987.

AUTHORS PROFILE

Among Top 3% Global Authors @SSRN, the former Director (HoPF) of LNJN National Institute of Criminology and Forensic Science of Ministry of Home Affairs, Government of India), Sandeep Mittal is presently a Joint Secretary in Parliament of India. He was a Member of Cyber Forensic Forum and Cyber Policy Working Group of Cyber Security Task Force of Data Security Council of India, an initiative of NASSCOM.

An "Ac-administrator" to the core, He is a postgraduate of Cranfield University, UK in Cyber Defense & Information Assurance and hold LLM of Strathclyde University, Glasgow in Internet Law & Policy. He is a Chevening Cyber Security Fellow, United Kingdom, Commonwealth Scholar in Internet Law and Policy, UK, an Associate of IDSA, New Delhi, Life Member of USI, New Delhi; IIPA, New Delhi; Indian Police Institute, New Delhi & Indian Society of Criminology, India.

Among Top 3% Global Authors @SSRN, the former Director (HoPF) of LNJN National Institute of Criminology and Forensic Science of Ministry of Home Affairs, Government of India), Sandeep Mittal is presently a Joint Secretary in Parliament of India. He was a Member of Cyber Forensic Forum and Cyber Policy Working Group of Cyber Security Task Force of Data Security Council of India, an initiative of NASSCOM.

An "Ac-administrator" to the core, He is a postgraduate of Cranfield University, UK in Cyber Defense & Information Assurance and hold LLM of Strathclyde University, Glasgow in Internet Law & Policy. He is a Chevening Cyber Security Fellow, United Kingdom, Commonwealth Scholar in Internet Law and Policy, UK, an Associate of IDSA, New Delhi, Life Member of USI, New Delhi; IIPA, New Delhi; Indian Police Institute, New Delhi & Indian Society of Criminology, India.

