



Aalborg Universitet

AALBORG UNIVERSITY
DENMARK

A Survey of Privacy Awareness and Current Online Practices of Indian Users

Motivating and Mitigating Factors for Improving Personal Information Privacy

Dhotre, Prashant Shantaram; Olesen, Henning

Published in:
Proceedings of WWRF Meeting 34

Publication date:
2015

Document Version
Other version

[Link to publication from Aalborg University](#)

Citation for published version (APA):
Dhotre, P. S., & Olesen, H. (2015). A Survey of Privacy Awareness and Current Online Practices of Indian Users: Motivating and Mitigating Factors for Improving Personal Information Privacy. In *Proceedings of WWRF Meeting 34: Santa Clara, CA, USA, Apr. 2015*

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- ? Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- ? You may not further distribute the material or use it for any profit-making activity or commercial gain
- ? You may freely distribute the URL identifying the publication in the public portal ?

Take down policy

If you believe that this document breaches copyright please contact us at vbn@aub.aau.dk providing details, and we will remove access to the work immediately and investigate your claim.

A Survey of Privacy Awareness and Current Online Practices of Indian Users

Motivating and Mitigating Factors for Improving Personal Information Privacy

Prashant S Dhotre and Henning Olesen

Center for Communication, Media and Information Technologies (CMI)

Aalborg University Copenhagen

DK-2450 Copenhagen SV, Denmark

psd@es.aau.dk, olesen@cmi.aau.dk

Abstract—Today, users with their smart devices can communicate and access a wide range of services via the Internet to make their life easier. However, loss of privacy is becoming a major issue for architects or policy makers, accelerated by the rapid development of mobile and wireless technologies that eases the collection, storage, sharing, analysis, and manipulation of the individual's information. The main objective of this paper is to study the privacy perception and awareness of Internet users in an Indian context. Results of comprehensive survey with 297 users are presented, focusing on their perception and awareness towards personal information privacy (PIP). The survey responses show that the user's perception is noticeably low considering PIP and that the privacy awareness is not the same as their understanding. The results indicate the need for a solution for PIP protection where the users have complete control over their personal information rather than the service providers, along with the establishment of a personal trust manager for building a trust between service providers and the individuals. The motivation and mitigation factors for such a system are analyzed and discussed.

Keywords—*perceptions; privacy; awareness; big data; personal attributes, privacy by design; personal information; awareness; and trust.*

I. INTRODUCTION

Mobile and wireless communication has brought many benefits for individuals, who are using their smart devices to make audio as well as video calls; staying in touch with friends and relatives, buying clothes and movie tickets, reading e-books while waiting for the train, etc. Our human lives are transformed because of the emerging technologies, providing huge benefits for our daily needs. However, the cost of using all these services is that service providers extensively collect and make use of our personal information. A huge variety of information is collected, stored, and processed without the user's consent, and our privacy is seriously at risk.

Surprisingly, today's most of the data are gathered within the last two years. For example, "There are 5 Exabytes of information created between the dawn of civilization through 2003, but that much information is now created every two days, and the pace is increasing"[1]. This is big data, defined as "any collection of large and complex data sets that are

difficult to process using on-hand database management tools or traditional data processing applications" [2].

Big data is characterized by high Volume, Variety, and Velocity, and some of its main challenges are the huge storage size required. The IT infrastructure should be capable of holding the different types of structured and unstructured data, and processing the big data to maximize its value for the business analytics. Adding the privacy perspective, another challenging component is to control and protect large sets of data containing sensitive and personal information.

In a web article from 2009 [3], the author described an interesting experience of his friend related to the protection of personal data, where his friend received a text message from a banking company with a credit card offer. Naturally, the surprised friend wondered how they got his contact number and the credit related information. Today, this has become big business, and data brokers are constantly collecting lists of people with detailed personal characteristics and selling them to other companies for targeted advertising. Are we really providing our information to these companies is the question to be asked? Access, disclosure, and misuse of personal information about individuals, are a key motivation for this research.

The paper is organized as follows: The motivation for conducting the survey and an example of privacy breach is described in Section II. The section III describes the work contribution towards the personal information privacy mechanism. The survey conduction along with its methodology is described in section IV. The important findings and results are discussed in section V. The paper is concluded in section VI.

II. TERMS AND MOTIVATION

The privacy design goals can be expressed as follows [4]:

"The goal of flexible, use-centric identity management infrastructure must be to allow the user to quickly determine what information will be revealed to, which parties and for what purposes, how trustworthy those parties are and how they will handle the information

and what the consequences of sharing their information will be”.

The Information Technology Act 2000 [5] defines the following terms:

- *Access*: “With its grammatical variations and cognate expressions means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network”.
- *Electronic Record*: “means data, record or data generated, image or sound stored, received, or sent in an electronic form or micro film or computer generated micro fiche”.
- *Information*: “Includes data, text, images, sound, voice, codes, computer programmes, software, and databases or micro film or computer generated micro fiche”.

Today, a huge variety of information is being collected, stored, and processed without the user’s consent, and our privacy is seriously at risk. Using ‘Big Data’ techniques [1] hidden patterns can be revealed, and additional value can be extracted from the data, giving rise to serious problems with leakage of our personal data. The effects of the privacy breaches range from professional to personal. Here, is one of the possible scenarios:

Mr.Sudhir is a nice, employed person. Unfortunately, he is suffering from a serious disease (like AIDS, influenza) at the age of 26. He consulted many doctors, but nothing worked well. One day he came across a health-related website, where all sorts of patients are connected and communicated to help each other. Mr.Sudhir thought it was a good idea to join and share his biggest problem for recovery. Few months later, his friends, and colleagues started to go away from him. The company asked him to resign and in his personal life, he lost his marriage proposal. Mr.Sudhir was shocked because of this. One day he saw that his disease details along with personal information (name, location) had been disclosed on a social site to, which his friends were connected. He is still wondering how his personal information was leaked?

To address the privacy issues in big data (“big privacy”) [6], it is important to develop a system for individuals, which can help them to control and manage the access to their personal data. In the proposed system, big privacy can be achieved by enabling the minimal and required disclosure of information, while accessing any service from smart devices. Embedding privacy at the design phase (“Privacy by Design” or PbD) [1] will be the basic principle on which the data security can be provided, and the privacy will be protected. The user will have more control over the personal information by means of providing the options like control and consent for usage in a secure way. In order to realize this goal, state-of-the-art technology for fine-grained attribute control will be researched and applied.

Hence, considering the Information Technology Act 2000 and the above-mentioned cases, it was decided to conduct a major survey of privacy in India. The principal objective of this survey was to determine Indian citizens’ awareness and understanding of privacy issues.

III. STATE-OF-THE-ART TECHNOLOGIES AND FRAMEWORKS

When we interact with service providers or other entities on the web, we disclose some of our personal attributes. In the digital world, the claims-based digital identity can give an insight of privacy to the users and prevent loss of trust with the help of digital identity[7].

The new strategy is focusing on the user level and the user’s choices for solving the privacy problems and securing our digital identities[8]. Privacy Enhancing Technologies (PET) is focused on risk elimination, empowering user-centric control, and access to information[9]. Kim Cameron’s Laws of Identity[7] emphasize on user’s minimal information disclosure with constraint, user consent, and communicating party awareness. The US government has presented NSTIC (National Strategy for Trusted Identities in Cyberspace) for the prevention of costly crimes and the execution of a secure transaction [10].

For a protection of privacy and dynamic profile creation, an identity layer is essential. OpenIDConnect builds on OAuth 2.0 [11] and focuses on identity interaction via REST (REpresentational State Transfer) [12]. It provides authentication, authorization, and attributes transmission capability. Another authorization protocol UMA (User Managed Access) developed by a working group under the Kantara Initiative addresses access control based on OAuth 2.0 [13]. Still, there is a scope for a generalized mechanism for resource protection. However, user expectations and experience must be considered in the creation of trust levels (Ranking of trust depends on the user’s preferences and experience). Microsoft has contributed in privacy protection by developing tools like Windows CardSpace[14], InPrivate[15], and U-Prove [16]. The important note is that the present solutions may be suitable for big organizations rather than on a personal/individual level.

The ongoing research addresses Big Privacy and the Personal Data Ecosystem (PDE) based on Privacy by Design (PbD)[17]. The seven architectural elements for this are: Personal cloud, semantic data exchange, trust framework, identity and data portability, data-by-reference or subscription, accountable pseudonyms, and contractual data anonymization.

When the user is online and is sharing sensitive information, most of the users don’t know the possible risks involved [18]. The purpose of mining users’ data by the external entities can be like fishing, spamming (bulk messaging), advertising and increase in the business, provide better services, and understanding the users interest [19]. There are some tools and algorithms available to find and make privacy settings [20]. Privacy plug-in designed for browsers are developed by Electronic Frontier Foundation (EFF) help

users to block tracking from third parties [21]. LightBeam browser plug in from Mozilla [22] enables the user to watch who is tracking them. The first and third party interaction is graphically represented in LightBeam. On the similar line, Online Permission Technologies has provided online privacy guard called MyPermission for Android and Apple devices [23]. MyPermission allows a panel for users to handle all service permissions.

Most of the survey based research work has been done considering the social networks. The Cheung [24] has mentioned the factors that force the students to use and share personal information on a social networking site like Facebook as it influences more than Twitter to youngsters. A survey was conducted by Goel et al. [25] for 400 social networking site users to know privacy issues, risks, and the user's online behavior.

The challenges in big data include the protection of personal information (name, date of birth, location, address), user's control over personal information and its misuse, processing and sale of personal information, location disclosure, data loss, and leakage[26]. In today's era of Internet, the privacy is more diversified, as it is not restricted to physical privacy only. The privacy of personal information is critical as a service provider uses personal identifiable information of the users for their/his own purposes. This implies that the user needs to give up personal information to the service providers to use all the provided services. However, the next question is how safe and private are our data with these service providers/websites?

IV. SURVEY AND METHODOLOGY

In the following subsections, we focus on the survey and the way it has been executed.

A. Design Principles of the survey

Most of the times, responding to a survey is ignored or finished over. To avoid this, it is important to follow design principles. According to [27], the survey must be simple to use. The questions should be a combination of multiple choices, scaling from 0 to 10, space for typed response, and some optional. The question should ask for personal information like cell phone, salary, etc. Also dividing the questions into a number of sections will create an interest among the participants. Also the objective/purpose and use of feedback must be stated clearly. Also, putting the interesting questions and gathering the feedback online is the efficient way of survey execution.

B. Protection Laws in India and Denmark

The Danish Act on Processing of Personal Data [28] [29] and the Indian Information Act 2000 [5], provide guidelines for when and how personal information should be processed for manual handling as well as on the Internet. However, there are cultural and acceptance barriers in countries like India with user-centric, user-controlled, and consent-based functionality. Hence, personal privacy protection is very important. The

developing countries like India have certain laws and rights like the freedom to talk and express. However, there is no law for the protection of PIP. In case of a wrongful collection, misuse and sharing of personal information, the Information Act 2000[5] talks about the possible sanctions.

C. Internet users taxonomy in Indian context

The Internet has turned out to be an internal part of present life. The increase of Internet use is not an exception for India. The population of India is estimated to be over 1.27 billion (year 2014) [30]. In India, it's found that more than 50% of the population is below the age of 25 and at least 65 % of the population is below at the age of 35. It is estimated that, an Indian's average age will be 29 years in the year 2020 as compared to China (37 years) and Japan (48) [31]. Penetration of the Internet is not an exception for India. India, the second most populous country in the world, has approximately 215.6 million Internet users in the year 2014, and this is likely to go beyond 346.3 in the year 2018[32]. Also, it is found that 37% of Internet users fall in the age group of 15-24 where as 38% are in the age group of 25-34. This distribution of Internet users in India shows that the maximum users are young having an age between 15 and 34. In view of the power of the Internet, the young men of India are not behind considering e Internet users. The Fig. 1 shows the demographics segment of active Internet users in India [33].

The largest set of Internet users is Youth (college going students). Considering the profile of Internet users in India, and to understand the privacy rights and issues, any survey has to target the college going students and young men having an age from 18 to 35 years.

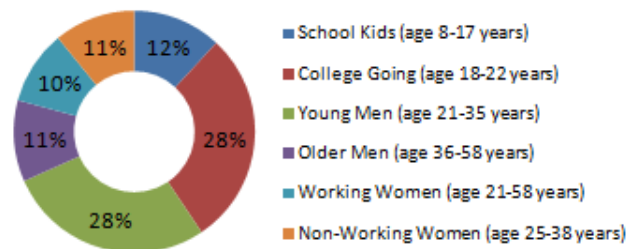


Fig 1: Internet user's taxonomy in India

Considering such a large number of users, there can be access, collection, misuse, and sharing of personal information by the different service providers/websites. There is no law that exists in India for the protection of personal information when there is stealing of personal information. Considering India's poor record in the protection of information privacy, the authors have decided to know the privacy awareness and suggestions on PIP from Internet user's in the Indian context.

D. Design of survey questions

The aim of the survey mentioned in this paper is to understand the user's knowledge on privacy and their awareness; to study the user's online practices. Also, this

survey aims at the users view on genetic information and privacy; impact of the user's online activities and behavior on their privacy. Equally, it is also important to check the user's attentiveness on privacy laws, policies, and duties of service providers.

The questionnaires were divided into the following sections:

- Your Current Practices
- Your Awareness about privacy
- Are you Serious when you are online?
- Your Online Activities
- Your Behavior
- Privacy Policies And Laws
- Your Organizations/Service Providers
- User on Mobile and Medical and Health Information.

The outcome will identify the possible threats, the user's privacy knowledge, and Internet activities/practices. Also, the suggestive responses on the asked questions will help to understand the motivations and mitigation plan for the protection of personal information privacy.

The questions were multiple choices, yes/no, and five point scaling questions. It's important to say that the percentage for a survey result may not add up to 100 because of rounding.

E. Survey Methodology

The methodology for the conduction of this survey comprises of online questionnaires and an interview mode. The questionnaires were created and made available online for a respondent instead of using the traditional offline method. This is achieved using Google Forms provided by Google. The online question can be seen at <http://goo.gl/forms/ctCImSfWHH>. Google Form link emailed to possible users available with the author's contact list. The author has published the online survey questions link to a set of users (group).

Even the link is made available to the groups that are available on networking sites (Facebook groups, Google groups etc.) to, which the author is connected already. The reason of selecting the Facebook and Google groups was the single mail containing the link for questionnaires that will reach the maximum users and will save the time that will take to send the mail individually. Similarly, an invited user can pass the link to the other users who may be the author's known or unknown users. However, the author has used the responses from his own organization and the other organization.

The focused users were public as well as private users. The public users are invited for the survey participation by those who were available on social websites. However, the survey was taken for the private users. However, the author has conducted the survey in his and the other private organization. The private users were the few students and the employees from the same organization as the author belongs to. Also, there are few users from the organization like IT companies, owned organizations, government sector, private organization etc. Despite the type of the users and their profession, the

focus of the survey was on individual's privacy awareness. This implies that the author has taken care about public users and private users for the survey.

At the other side of the online survey questions and interviews had been conducted by the author. One of the reasons for taking an interview is to know the views on privacy and get extra information apart from the important findings from the survey. Also, during interviews the author has the chance to observe the users feelings, body language, gestures, and postures. The respondent's intentions of behind answers and their expressions can be more communicative and meaningful. Such expressions and additional information can't be obtained from the survey questions.

To understand the user's awareness towards personal information privacy and their feedback on present privacy systems, a survey was conducted at the national level. Total 297 users (205 Male, 81 Female and 11 non-specified) responded to the survey. The survey was conducted from October 10th to November 05th 2014 across different regions/locations of India. The survey was executed for the citizens of diverse age, gender, and profession. This diversity is considered and needed to get the actual and correct feedback. The survey has covered all types of users so that no particular group is missed.

F. Data Analysis

All the responses were collected in a spreadsheet. For the analysis of the survey responses, the authors have decided to select the business intelligence tool called Tableau [<https://www.tableausoftware.com>]. This tool is available in different versions like public, desktop etc. The authors have used a desktop trial version, which was free for 15 days and then the public version of the same tool.

This is a free tool to download and use. There is no need for programming skills to use it. The authors have experienced that this tool is simple and allows obtaining the results using the drag and dropping process on the responses available in a spreadsheet.

V. RESULTS AND DISCUSSION

In the following, we focus on evaluation of survey responses, important finding and how motivation and mitigation factors help for designing privacy mechanism. A national level survey of the Indian citizens on PIP and other issues was conducted and 297 Indian residents submitted response to the survey. The male (72%) and female (28%) respondents shared answers to the survey questions.

Major distribution of respondents in terms of their profession is students and employees (part and full-time). Students (55%) and employed (36%) apart from other professions who participated in the survey. Similarly, Major distribution of respondents in terms of age is Between 16 and 25(76%), between 26 and 35(17%), between 36 and 45(4%). The rest of the age distribution is less than 1%.The maximum responses received from respondents of age between 16 and

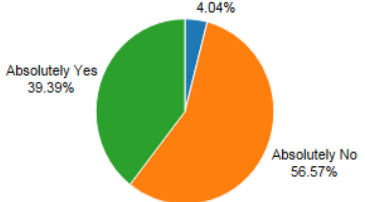
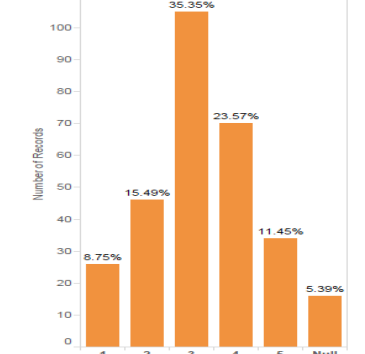
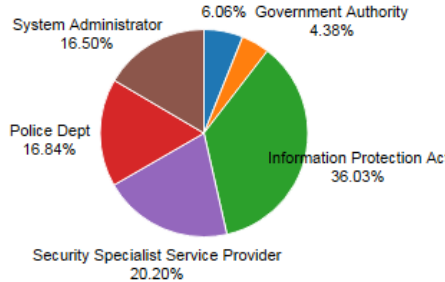
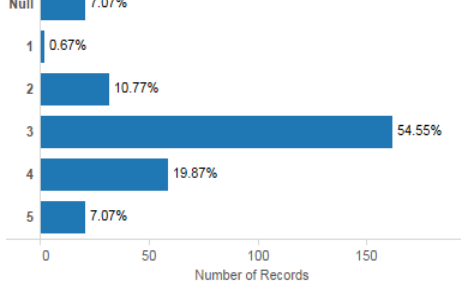
35. The survey conducted for the users of different age, gender, profile and profession. The responses of survey are discussed in following subsections.

4. Understanding, perception and awareness of privacy:

This section focuses on the participant’s responses of those questions which were based upon to know their understanding, perception and awareness of privacy. The first question in this

category was related to the kind of privacy they feel more important in their life. From the responses it may be an indication about anxiety of personal life of the respondents as compared to professional or social life. Almost 84% of the respondents feel the personal privacy is far important than the professional or social life privacy. The concerned responses are shown in Table I.

TABLE I. USERS UNDERSTANDING, PERCEPTION AND AWARENESS OF PRIVACY.

| Question | Participant’s Response | Description/Discussion |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 10. Do you know any national institutions/Law that will helps the Indian users to deal with user’s privacy along with their identifiable information protection from wrong way of information collection, its utilization (use) and sharing options? |  <p>Fig 2: Users knowledge on national privacy law</p> | The national institutions/law provides helps to the respondents in the case of privacy rights or privacy breach. Fig. 2 represents that almost 57% participants of this survey do not know laws or national institution that helps the users for protection of personal information privacy. |
| 11. What would you think about your knowledge level for your privacy rights coming under the personal information protection laws? (1= Very high, 2=high, 3=poor, 4= very poor, 5= don’t know). |  <p>Fig 3: Users knowledge on privacy rights</p> | Answering to five points scaling question, the respondent’s knowledge on privacy rights is high or very high among just 25% of total respondents. It clearly denotes that the 75% said, their knowledge was found to be on lower side as shown in Fig. 3. |
| 44. Where do you ask a question if security / privacy is breached? |  <p>Fig 4: Respondents view on privacy breach resolvers</p> | If the privacy is leaked, perhaps the respondents are puzzled. Fig. 4 illustrates 36% say that they will use Information Protection act for the protection of their privacy. 16.5% respondents will consult with their system administrator whereas 17% would go to the police department for getting fairness on the privacy loss. The security specialist will be called by 20% of the participated respondents. The least (4%) will ask the government authorities for their privacy losses. |
| 46. How do you rate the present privacy system as per your experience while dealing with service providers? (1 best, 5 worst) |  <p>Fig 5: Rating of present privacy system</p> | The respondents are not satisfied with existing/present privacy system. Fig. 5 depicts that respondents believe that there is a necessity for an improvement in the privacy system. Based upon the user’s experience the 11% of the respondents are satisfied with the present privacy system which is very low. 82% of the respondents are rating their experience with present privacy system as “neither good nor bad, bad, or very bad”. |

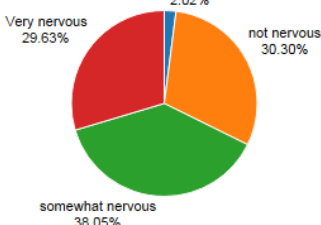
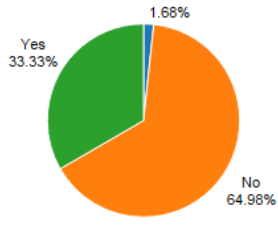
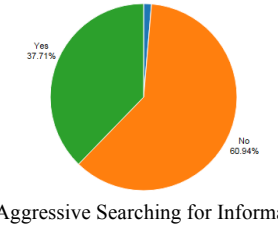
Also, answering to the most serious risk to your privacy, it is observed that the most concerned issue are bank/finance fraud and access or process of personal information as compared to Computer security/privacy, Identity fraud/theft, activities related to user monitoring and tracking and health related information. Cell phone privacy is least concerned. This is a sign of user's concern about personal information

and online activities. The concerned responses are shown in Table I.

B. User's Internet activities and online practices:

To understand the user's Internet activities and online practices, following few questions were asked during the survey. This sections discuss on the respondents view and practices whenever they are online and is summarized in table II.

TABLE II. USERS INTERNET AND ONLINE ACTIVITIES.

| Question | Participant's Response | Description/Discussion |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>21. Marketing companies use your personal identifiable information to analyze your opinions (For example: likes/Yes, dislikes/No).</p> |  <p>Fig 6: Respondents view on information collection by marketing companies</p> | <p>The use of likes and dislikes of participants is a worried issue for them indicates strong understanding of the marketing strategies of companies. Fig. 6 says 68% of total participants are somewhat or very nervous about the usage of user likes and dislikes. The usage of likes and dislikes is expected to be clearly specified by companies so that the user will be aware of it.</p> |
| <p>26. Do you take any steps/actions to limit tracking/monitoring of Internet/online activities?</p> |  <p>Fig 7: Users actions to limit tracking of online activities</p> | <p>The participants are uncertain to take any strong steps so as to limit the tracking or monitoring of the user's internet/online activities. Almost 65% of the total participants do not take strong steps for limiting such online activities as shown in Fig. 7.</p> |
| <p>14. Have you aggressively searched for information on your privacy and concerned rights? Like an example: visiting a related website, searching on the internet, contacting an agency / organization, or taking a review a standard publication for desired help?</p> |  <p>Fig 8: Aggressive Searching for Information on privacy</p> | <p>Most of the respondents were not actively hunted for information on privacy issues and concerned rights. Fig 8. illustrates, almost six out of ten respondents do not know where to look for information on personal privacy rights. Statics from fig 8 forces to have a mechanism in future, where user can track the information about the privacy and concerned rights.</p> |

C. Unwillingness to share personal information:

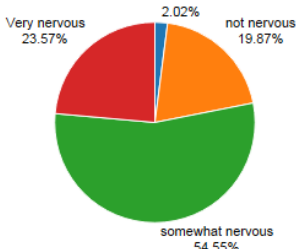
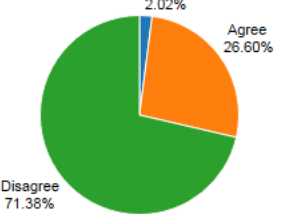
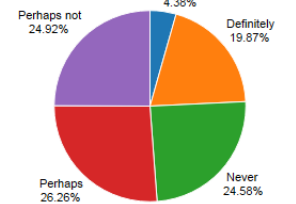
There has been always a tradeoff between user's privacy and services offered by service providers. To understand the users concerns when they have to reveal information to get services from service providers.

For a question, "Would you like to disable the location disclosure option on your cell phone because you may feel

nervous about your location access?", the 68% of the respondents are concerned about their location information and hence turned off the location tracking options of their cell phones considering the access to their other information.

The Table III shows the users concerns and unwillingness to share personal information.

TABLE III. USERS UNWILLINGNESS TO SHARE PERSONAL INFORMATION

| Question | Participant's Response | Description/Discussion |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 19. Without a warrant, the law administration/national security agencies, collects it for general surveillance/investigation purposes (Very Nervous, Somewhat nervous or Not nervous). |  <p>Fig 9: Issue on Collection of Information by Security agencies</p> | Fig. 9 shows that 80% of the total respondents are concerned about collection of personal information by law administration/national security agencies for some investigation or surveillance purposes. In a broader perspective the user's privacy concerns and the enterprise security concerns are all a matter of managing. |
| 35. Content/service providers have the right to share/resell information about their users to other agencies/companies. (Agree or disagree) |  <p>Fig 10: Respondent's view on right to share/resell information</p> | The 71% respondents are strongly disagreeing on the rights of service providers for sharing or reselling about their information to other agencies. From Fig. 10, we observe that the user must have a control on their information. |
| 55. Would you fear to undergo genetic (medical) testing? |  <p>Fig 11: Users View on Genetic Testing</p> | The 46% respondents say that their concerns would influence readiness to undergo medical/genetic testing. Interestingly, almost 25% respondents not at all worried about medical or genetic testing as shown in Fig. 11. |

D. Privacy Policy:

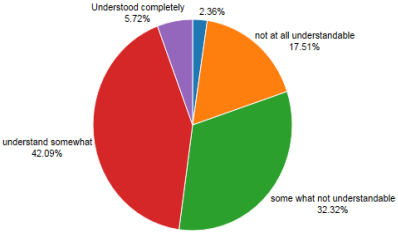
Privacy policy is an important as long as the relationship between user and service providers is concerned. To understand the users view on privacy and data policy of service providers, few following questions were asked in the survey. Table IV depict the respondents view on privacy policy in detail.

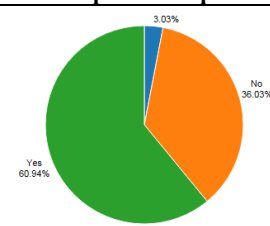
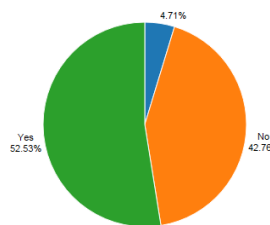
One of the questions was related to regularity of reading the privacy policy of websites/ service providers they visit (doing registration at least). The comprehensive analysis of the survey shows that the 76% respondents do the registration to the websites without reading the contents of privacy policies of the service provider/website. There are only 8%

respondents who continuously read privacy policy. This implies the unawareness about privacy policies.

To know the users view on privacy policies in terms of length, description and understanding, a question was asked. After analyzing the responses, it is found that 87% of the respondents believe that the privacy policies of the websites/service providers that they visit are lengthy, unclear. Most of the respondents say that the privacy policies are in imprecise or unfocused way. Also, they feel that the content of the policies are not able to understand. Other responses are shown in table IV.

TABLE IV. RESPONDENTS VIEW ON PRIVACY POLICY OF THE SERVICE PROVIDERS.

| Question | Participant's Response | Description/Discussion |
|----------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 40. How you find service provider's privacy policies about dealing with your personal information? |  <p>Fig12: Respondents view on service provider's policies</p> | Only 6% of the respondents who completely understand the privacy policies about the use of the collected information by the service provider. However, the majority (92%) of the respondents feel privacy policies are imprecise, unclear about what, when the information collect and what they will achieve from it. Fig 12 is an indication that the service providers should make clear and short privacy policies. |

| Question | Participant's Response | Description/Discussion |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 41. Have you come across any situation where you decided not to select a website or a service because you are unhappy with the terms that set in privacy policy? |  <p>Fig 13: Unhappiness of respondents on terms in privacy policy</p> | Considering the terms and conditions in privacy policy in discussion, 61% of the respondents decided not to select a service provider or a website. They believe that the policies are unclear and don't know how the information will flow from service providers. Fig. 13 illustrates six out of ten respondents are unhappy with the terms that are set in the privacy policy. |
| 42. If personal information is gathered over the Internet, do you know a specific policy to manage/storing and processing of your personal information? |  <p>Fig 14: Specific policy for handling personal information</p> | The 43% of the respondents are not aware of the policies to store, manage and process their information. However, the 53% respondents are aware of the about options/ways how to manage, store and process their information that has been collected by service provider/website. The individuals should have more options to control their information once it is available on Internet. |

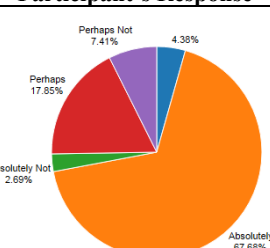
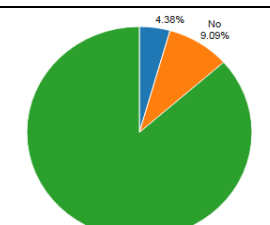
E. Mitigation Factors (Suggestive responses):

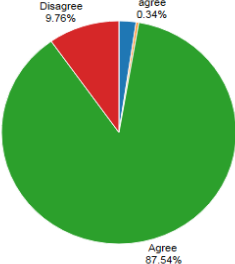
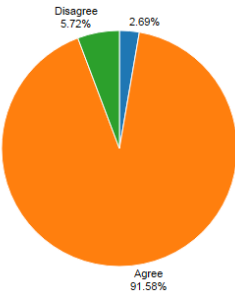
In the survey, some questions were put to understand and analyze users need for the protection of their personal information privacy. This section pulls towards mitigation factors for the improvement of personal information privacy. The suggestive responses are described in table v.

One of the suggestive responses on the new personal information protection law was collected. From survey

responses, it's prominently found that the 97% of the respondents believe to have a new law(s) for the protection of the user's information when they are performing some internet activities. It implies the risks are involved in today's internet, or there are the issues of internet security that to be addressed. Not only the banks or the firms, user's responses denote to have a personal information privacy law for everyone.

TABLE V. RESPONDENTS VIEW ON PRIVACY POLICY OF THE SERVICE PROVIDERS.

| Question | Participant's Response | Description/Discussion |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 27. Do you believe and think that the service provider/Internet organizations should request your consent to follow and observe your online/internet activities? |  <p>Fig 15: Respondents view on service providers consent before data collection</p> | The 86% of the respondents claim that the service provider/Internet companies must take user's permission to observe their online activities. The responses from Fig 15, denote the users are worried for hidden tracking mechanism adopted by service providers. |
| 47. Do you feel that the service provider should notify you when they deal (access, sale, share) your personal information? |  <p>Fig 16: Respondents opinion on notification by service providers</p> | In Fig. 16, the respondents are showing inclination towards more openness between the service providers and themselves. 87% of the respondents believe that the service provider must notify the users when they access, sale or share users information. |

| Question | Participant's Response | Description/Discussion |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 34. I support the establishment of a personal trust manager (where a trusted entity/party keeps my preferences/experience to build trust between me and the service provider) |  <p>Disagree 9.76% agree 0.34% Agree 87.54%</p> <p>Fig 17: Respondents view on the formation of personal trust manager</p> | The users are looking for a strong belief in the reliability and truth needed between the service provider and themselves. In Fig. 17, there are 88% respondents who demand for a "personal trust manager" in upcoming time. When the user is online, the preferences and the experience of the user must be observed and monitored by personal trust manager for building trust. |
| 36. A user should have complete control over which sites that collect the user's important and critical information. |  <p>Disagree 5.72% 2.69% Agree 91.58%</p> <p>Fig 18: Respondents view on control over on personal information</p> | The respondents believe that they should have the control over their personal information which has been collected by the service provider. As shown in fig 18, a strong claim made by 92% respondents for providing user control on the critical and important information. It implies to have a mechanism where the user can see how the service provider collects, use and share personal information in detail. |
| 48. Do you feel there should be a mechanism to rank the service provider/services according to your experience collection? For example, do you think the rating of ""how secure"" a specific site is helpful for you? |  <p>4.38% No 7.74% Yes 87.86%</p> <p>Fig 19: Respondents view on ranking of service provider</p> | The respondents are expecting an establishment of strong trust between the service provider and themselves. 88% respondents expect a mechanism that should tell them the rank/level of the service provider based on their experience. They believe such mechanism will help them to know how secure a specific site is. |

VI. CONCLUSIONS

In this paper, we evaluated the responses of the respondents of the survey in terms of user's privacy awareness, understanding towards privacy; user's Internet activities; user's reluctance to share personal information; user's understanding about privacy laws; and suggestive responses (mitigation steps) on a better privacy protection mechanism. The survey shows that the respondents have limited knowledge on privacy and the concerned laws. This implies that there is a lack of confidence, and there is a need of PIP awareness programme in India. Also, respondents don't know the place or organization to contact, if their privacy is breached. The participants strongly understand the marketing strategies of companies and are worried on their "like" and "dislike" options. The respondents believe that PIP is most critical issue to be faced by India in the next ten years.

Furthermore, the respondents are worried about collection of their personal information by law administration/national security or service providers. The respondents are very reluctant to disclose the personal information and nervousness while sharing medical/genetic information. Most of the

respondents are unhappy with the present handling of privacy. As long as information is stored online and digitized, the privacy protection mechanism should be proposed for securing the citizens' personal information. This is the motivation for building a new privacy system for the protection of personal information.

Respondents suggest that the service providers must take consent and provide notification whenever they deal with user's information. The users demand more control on their personal information instead of being controlled by service providers. Hence, there is a need of strong and firm personal information privacy law in India. The citizens, who want better privacy protection in relation to services, should be able to rank service providers depending on how they handle the user's preferences and context. The establishment of personal trust manager will help the users to build and manage trust levels for service providers/websites. There is still a lot of confusion, when the user deals with the privacy policies (terms of use) of the service provider.

In the future work, the authors will make a privacy policy analysis for different service providers and develop an

improved PIP system to assist users in managing their personal information and trust towards service providers.

VII. REFERENCES

- [1] Ann Cavokian, Jeff Jonas, "Privacy by Design in the Age of Big Data"[Online]. Available: http://privacybydesign.ca/content/uploads/2012/06/pbd-big_data.pdf. [Accessed: 18-Dec-2014].
- [2] 'Big data - Wikipedia, the free encyclopedia'. [Online]. Available: http://en.wikipedia.org/wiki/Big_data. [Accessed: 18-Dec-2014].
- [3] 'The Malaysian Bar - Putik Lada: Keep personal data personal'. [Online]. Available: http://www.malaysianbar.org.my/national_young_lawyers/putik_lada_keep_personal_data_personal.html. [Accessed: 18-Dec-2014].
- [4] Ann Cavoukian, ph.D. "Privacy in The Clouds"[Online] Available: <http://www.ipc.on.ca/images/resources/privacyinthecLOUDS.pdf> [Accessed: 21-Dec-2014]
- [5] "Information Technology Act, 2000"[Online] Available: http://www.dot.gov.in/sites/default/files/itbill2000_0.pdf [Accessed: 20-Dec-2014]
- [6] A. Cavoukian and D. Reed, "Big Privacy: Bridging Big Data and the Personal Data Ecosystem Through Privacy by Design," 05-Dec-2013. [Online]. Available: http://www.privacybydesign.ca/content/uploads/2013/12/pbd-big_privacy.pdf
- [7] "The Laws of Identity" - [Online]. Available: <http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf> [Accessed: 19-Dec-2014].
- [8] 'The Laws of Identity'. [Online]. Available: <http://msdn.microsoft.com/en-us/library/ms996456.aspx>. [Accessed: 18-Dec-2014].
- [9] 'NR publication | Norsk Regnesentral'. [Online]. Available: http://www.nr.no/en/nrpublication?query=file/PETweb_D2-1_StateoftheArt_PET_Report.pdf. [Accessed: 19-Dec-2014].
- [10] 'President Obama Releases the National Strategy for Trusted Identities in Cyberspace | The White House'. [Online]. Available: <http://www.whitehouse.gov/blog/2011/04/15/president-obama-releases-national-strategy-trusted-identities-cyberspace>. [Accessed: 19-Dec-2014].
- [11] "OAuth - The Big Picture," *iBooks*. [Online]. Available: <https://itunes.apple.com/us/book/oauth-the-big-picture/id515116202?mt=11>. [Accessed: 21-Jun-2014].
- [12] "OpenID Connect | OpenID." *Online+. Available: <http://openid.net/connect/>. *Accessed: 30-Jun-2014].
- [13] "Home - WG - User Managed Access - Kantara Initiative." *Online+. Available: <https://kantarainitiative.org/confluence/display/uma/Home>. [Accessed: 21-Jun-2014].
- [14] "Introducing Windows CardSpace." *Online+. Available: <http://msdn.microsoft.com/en-us/library/aa480189.aspx>. [Accessed: 21-Jun-2014].
- [15] "InPrivate-browsing - Microsoft Windows," *windows.microsoft.com*. [Online]. Available: <http://windows.microsoft.com/da-dk/internet-explorer/products/ie-9/features/in-private>. [Accessed: 21-Jun-2014].
- [16] "U-Prove Microsoft Research," Online. Available: <http://research.microsoft.com/en-us/projects/u-prove/>. [Accessed: 23-Aug-2014].
- [17] Ann Cavokian, Drummond Reed, "Big Privacy: Bridging Big Data and the Personal Data Ecosystem Through Privacy by Design". [Online]. Available: http://www.ipc.on.ca/images/ResouRces/pbd-big_privacy.pdf. [Accessed: 28-June-2014].
- [18] J. L. Becker and H. Chen, "Measuring privacy risk in online social networks," Ph.D. dissertation, University of California, Davis, 2009.
- [19] M. Huber, M. Mulazzani, E. Weippl, G. Kitzler, and S. Goluch, "Exploiting social networking sites for spam," in Proceedings of the 17th ACM conference on Computer and communications security. ACM, 2010, pp. 693–695.]
- [20] J. L. Becker and H. Chen, "Measuring privacy risk in online social networks," Ph.D. dissertation, University of California, Davis, 2009.
- [21] Electronic Frontier Foundation (EFF) – "Privacy Badger" <https://www.eff.org/privacybadger>, 2014
- [22] John-David Rusk, Trust and Decision Making in the Privacy Paradox, SAIS 2014 Proceedings. Paper 32. <http://aisel.aisnet.org/sais2014/32>
- [23] Online Permissions Technologies, "MyPermissions - online privacy shield", <http://mypermissions.org/>.
- [24] Cheung, Christy MK, Pui-Yee Chiu, and Matthew KO Lee, "Online social networks: Why do students use Facebook?" in Computers in Human Behavior, vol. 27, pp. 1337-1343 2011
- [25] Ms. Shivi Goel, Dr. Sanjeev Dhawan, Dr. Kulvinder Singh, "Impact of Privacy Attitude, Concern and Awareness on Use of Online Social Networking", 5th International Conference- Confluence The Next Generation Information Technology Summit (Confluence) vol. pp.14-17.
- [26] P. Gundecha and H. Liu, "Mining social media: A brief introduction." Online: Available: http://www.academia.edu/2931894/Mining_Social_Media_A_Brief_Introduction. [Accessed: 04-Mar-2015]
- [27] Nelson Norman Group. "Collecting Feedback From Users of an Archive (Reader Challenge)" Online. Available: <http://www.nngroup.com/articles/collecting-feedback-from-users-of-an-archive-reader-challenge/>[Accessed: 04-Mar-2015]
- [28] "The Act on Processing of Personal Data." [Online]. Available: <http://www.coe.int/t/dghl/standardsetting/dataprotection/national%20laws/DANEMARKThe%20Act%20on%20Processing%20of%20Personal%20Data.pdf>[Accessed: 21-Jun-2014]
- [29] 'Datatilsynet: Compiled version of the Act on Processing of Personal Data'. [Online]. Available: <http://www.datatilsynet.dk/english/the-act-on-processing-of-personal-data/read-the-act-on-processing-of-personal-data/compiled-version-of-the-act-on-processing-of-personal-data/>.
- [30] "Demographics of India-Wikipedia" Online+. Available: http://en.wikipedia.org/wiki/Demographics_of_India#Population_above_the_age_of_7. [Accessed: 04-Mar-2015]
- [31] "U.S. Relations With India" Online. Available: <http://www.state.gov/r/pa/ei/bgn/3454.htm> [Accessed: 04-Mar-2015]
- [32] "Number of Internet Users in India-Stastica.com Online. Available: <http://www.statista.com/statistics/255146/number-of-internet-users-in-india/>. [Accessed: 04-Mar-2015]
- [33] "Internet in India 2013" IMAI I-CUBE 2013 Online. Available: http://www.imrbint.com/downloads/Report-BB55685%20IAMI%20I-CUBE_2013-Urban+Rural-C1.pdf [Accessed: 04-Mar-2015]