Data Protection Guidelines for Protecting Privacy of Users on Social Media

Fatema Panvelwala
Master of Computer Applications
Veermata Jijabai Technological Institute

Archana G. Pai
Assistant Professor,
Master of Computer Applications
Veermata Jijabai Technological Institute

ABSTRACT
Social Media interaction is growing at a rapid pace. Every smart phone user has at least 1 social media account. Social media websites offer th*eir users what seem like free services. These free services are then paid for in kind when the social media websites use their personal information to aide their business objectives. In this paper, I have included survey results of a user awareness survey that I conducted among people from various demographics. The total number of respondents to that survey was 404. I have used Facebook as the subject of my survey and will be using the results to generalize to other social media websites. The survey showed that people are ignorant of the ways in which their personal data might be misused.

Another section of my paper will consist of a summary of our current IT Act, its limitations in extending their jurisdiction to OSNs (Online Social Networks) and a growing need for India to have a dedicated Personal Data Protection Act. Lastly, I would like to propose some framework or guidelines on which our Personal Data Protection Act can be compiled.

Keywords
Privacy, data protection, user awareness, IT act, Social Media

1. INTRODUCTION
Internet is omnipresent in this new and modern world of technology. We now live in a world where the number of devices connected to the internet is outnumbering the total population of earth. People spend more time updating their social media statuses than in connecting with people in the real world. Social media has become an addiction among the users. All such websites offer free networking services to their users to stay connected with their friends and acquaintances as well as to make new friends.

However, as they say "there's no free lunch", these services that appear to be "free" are not really free services. Andrew Lewis rightly said "If you are not paying for a service, then you are the product not the customer". When social media websites offer you free registration, they are hoping to get revenue in some way or the other. The most innocent of these is to show you advertisements that you might be interested in. Another way is that they share your personal information by their 3rd party entities.

Recent advancements in data analytics has made it possible to make the most out of advertising by doing what they call "targeted advertising".[1] Targeted advertisements basically mean that they use your personal data to create a profile of you and then show you advertisements for the products you are likely to be interested in. On the face of it, this does not seem scary or intrusive at all. Instead it feels as if the company is being thoughtful by presenting to you advertisements of products which you might be interested in buying rather than any other products that may be irrelevant. It can also be considered as, if they know what you might be interested in buying, they might be able to manipulate you into buying what they want you to buy.

Even worse is when the social media company tailors your newsfeed to suit what you want to believe instead of showing you all the stories. When you "like" a post on Facebook, or perform a similar action on some other website, any post or news article, you can be sure that you will see similar such articles from next day onwards. They try to trick you into believing that your opinion is the opinion of the masses. This is very dangerous as it can manipulate the users into believing a lie and sway public opinions.

Incidents like these occur because of 2 main reasons. One is that users are not aware that social media websites can use their information for these business agenda. Ignorant users provide the social media websites with access to their personal data and rights to access them without knowing. The other reason is that there are no regulations that maintain a check on these websites. There are no Personal Data Protection Laws in India that can regulate these websites.[2] And so, the social media websites can freely do their work and then claim that they never forced anyone to join their website, and that the users themselves gave us access to their data.

This present state calls for a need for some law or guideline for the social media networks that can regulate the policies of such websites. Such laws do exist in other countries, and it is time India too made such a law.

2. WHAT HAPPENS WHEN YOUR DATA IS LEAKED?
As users are spending more and more time on the social media websites, they keep adding to their personal information on the OSNs. A breach of security on part of the OSNs can lead to a breach of the user's privacy and have unwanted consequences. A data breach may lead to:

- **Illegal advertisements and manipulation**[3] – people unknowingly become victims of targeted advertising. These advertising agents may have obtained their personal data illegally, which is a breach in their privacy. The advertisers then keep sending them advertisements in the form of text messages and emails which spam the users. A lot of advertisements about a particular product might also manipulate the users into buying the product or falling into traps.
- **Ideological manipulation** – People get influenced by posts they see on social media. In such a case, it is easy to manipulate people by putting them in contact with certain posts that can make them influenced in a certain direction. This is dangerous

as it can be used to manipulate a user's opinion in political matters and influence the opinion of the voters on behalf of particular politicians. A fairly recent incident that happened was when Cambridge Analytica, a data analytics firm tried to obtain data about users from Facebook. Cambridge Analytica arranged a process to obtain consent from users to participate in a research by filling out a survey. Facebook allowed this app to not only collect the personal information of people who agreed to take the survey, but also the personal information of all the people in those users' network.[4]

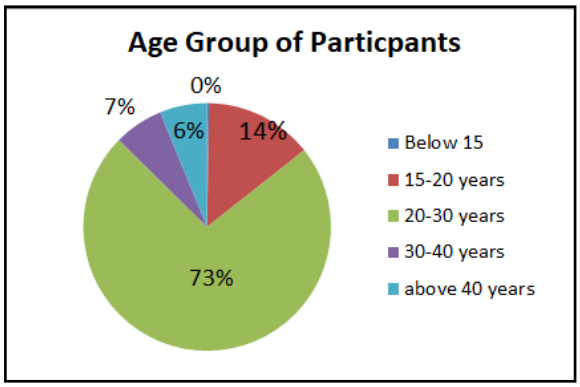
- **Government spying** – government can obtain information about individuals easily from social media websites.
- **Stolen Identity** – data leak can lead to people masquerading as other people. It would be very easy to take place of an obscure, unknown person if one knows enough information about that person and can go unnoticed for a long time. It has also become very easy to obtain such information in India as we see many breaches in Aadhar data.[5]
- **Phishing** – Phishing is when a user receives emails from seemingly genuine sources and asks users to enter their personal information. If an attacker obtains leaked data of the users, it can pose as their bank website and make users enter their sensitive bank details on the page thereby giving the attacker access to their bank accounts. A recent incident was when users of a Canadian bank received custom crafted emails that looked exactly like the legitimate website. This affected lot of bank users.[6]

3. USER AWARENESS SURVEY

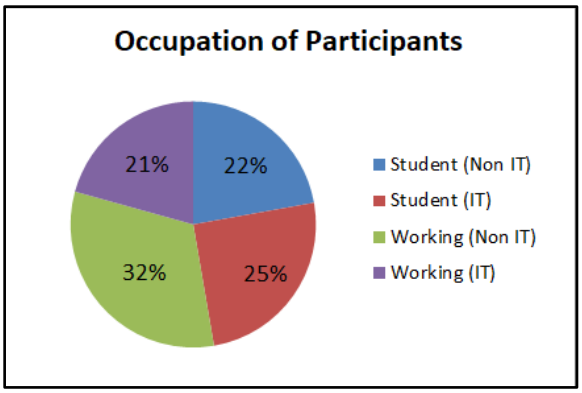
When users put their information on the social media websites, they feel that only users they have approved – (friends on Facebook, followers on twitter, Instagram) can have access to their information, but there is someone else they forget to factor in - The OSN itself. The OSN has information about all the users and all their actions. The main reason people don't consider data in the hands of OSN as insecure is because they are not aware. Users of OSN do not know that the OSN has the right to use their data for advertisements and showing them "relevant content" among other things.

To assess the level of awareness among the users, a survey was conducted via Google Forms. 405 people participated in the survey. The demographic of the respondents can be summarized by the following charts.

The participants belong to all age groups with the highest number being from the range of 20-30 years

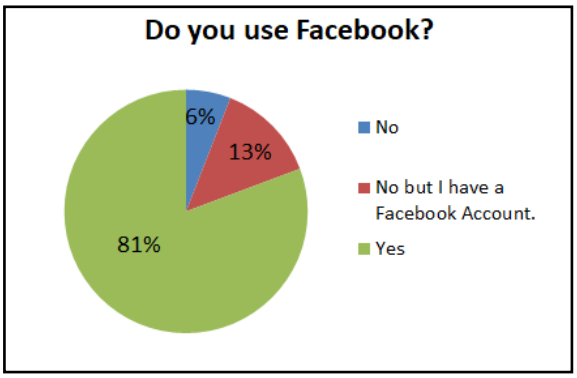


(Figure 1)



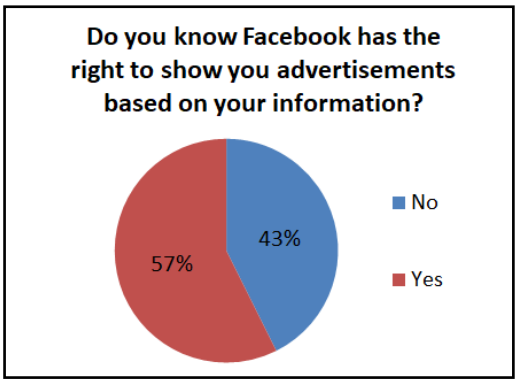
(Figure 2)

Among the respondents surveyed, 81% people use Facebook actively. And another 13% respondents do have an account on Facebook, even if they do not use it. Further survey was conducted on these 94% respondents.



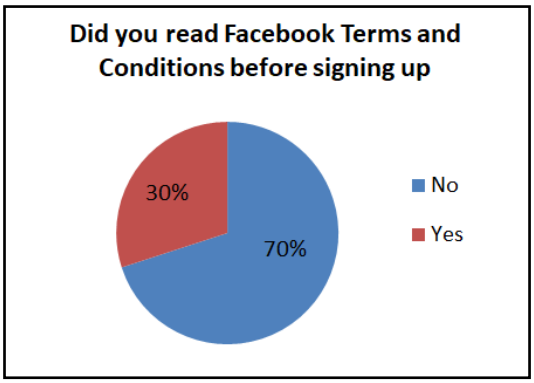
(Figure 3)

When asked about whether they know that the Facebook has the rights to use their information to show them advertisements, 43% responded in negative.



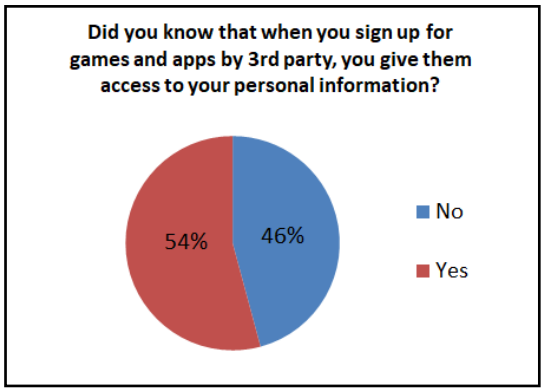
(Figure 4)

This lack of awareness of users can be attributed to the fact that users don't read the Terms and Conditions of the OSNs before signing up on them. A massive 70% respondents said that they did not read the terms and conditions of the OSN before signing up.



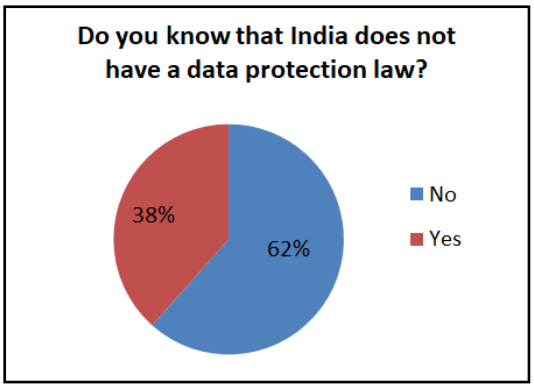
(Figure 5)

Facebook has some 3rd party applications and games that users can use by signing up with their Facebook accounts. This allows the 3rd party application access to the users that sign up for them. When users were asked whether they knew that those 3rd party applications could access their personal data, 46% users said that they did not know that.



(Figure 6)

Also 62% users are unaware that India does not have a dedicated data protection law that would help them in case of any violation of their privacy.



(Figure 7)

4. ANALYSIS OF THE SURVEY

From the result of the survey, it can be observed that:

- 94% people use Facebook or at least have a Facebook account
- Most of these users provide their personal information on Facebook.
- More than 40% users do not know that Facebook uses their personal data to show them advertisements and other "relevant" posts.
- Around 70% users do not read Terms and Conditions before signing up on Facebook
- Users signup for 3rd party applications on Facebook, but they do not know that those 3rd party applications also get access to users personal information.
- 62% do not know that India does not have a dedicated data protection law.
- Users who are studying or working in the field of IT are also not more aware or cautious on Facebook than the non IT ones.

5. EXISTING LAWS

People think if they are on the right side of the Law, then the Law will help them. However, in the case of their privacy on social media, the law won't be able to help them much primarily because India doesn't have a dedicated data protection law. The constitution of India does not explicitly guarantee a right to privacy, but it is implied from Article 21 which states that "no person shall be deprived of his life or personal liberty except the procedures established by law". Here, personal liberty is extended to imply a life free from any encroachments that is unsuitable in law. However, the fundamental rights can only be invoked against the state or state owned enterprises and not against any private individual.

Some sections of IT Act 2000[7] that are related to data protection are:

- **Section** 43A – It states that any corporate body that stores information in their private databases, and fails to implement necessary security which leads to wrongful gains or loss to any person, will be held liable to pay for the damages
- **Section 72A** - Punishment for Disclosure of information in breach of lawful contract – any person or entity that discloses the personal information about any individual shall be held liable and can be imprisoned or fined.
- **Section 69** – This is an exception to the above rules. It states that the state has the right to breach an

individual's privacy if it is in the interest of the security or defence of the state.

In 2011, an amendment to the IT Act was made, in which the term "sensitive data" was given a formal definition. It defined personal data as – "information including but not limited to – passwords, financial statements, physical or mental health conditions or biometric information."

In 2013, a Personal Data Protection Bill was proposed that would safeguard the interests of private individuals regarding their personal information.[8] This Act, when it came into force would have overridden the existing IT Act. Section 3 of the Act states that "*no person shall collect, store, process, disclose or otherwise handle any personal data of another person except in accordance with the provisions of this Act an d any rules made thereunder.*"[9] However, the bill has not been passed till now due to 2 main reasons:

1. Disagreements between judiciary and intelligence agencies – The intelligence agencies argue that they need to get access to personal information of the citizens to provide better security.
2. There is a debate over whether the law should be applicable to all the residents of India or to only citizens of India.

The second issue was solved in the 2014 draft of the bill which stated that the law would extend to residents also but this draft is not publicly available.

This Act, if it came into force, would be more transparent than the IT Act. It provides guidelines for lawful processing of data as well as provisions for the intelligence agencies. However, this will again not be very effective for regulating user's personal data on social media websites.

This lack of a dedicated data protection act also affects adversely on the foreign companies that intend to do business with India.

6. PROPOSED GUIDELINES FOR DATA PROTECTION BILL

6.1 Data Collection

The OSN should not be able to collect the data of the users if the user is not logged in to their website.

a. An OSN should not be legally allowed to gather user data when they are not actively logged in to the OSNs service.

b. The data collection from cell phones should also not take place when the users OSN app is not in use or even in background.

c. The user should have the right to know what data is being collected about them.

d. The OSN should not be able to collect any data of users that have not signed up to their service or have unsubscribed or deleted their accounts.[10]

e. It should not be acceptable for OSN to record users conversations through a microphone or camera when the user is not explicitly using them.[11]

f. For mobile applications, a check should be maintained for the permissions required by the application. Some applications refuse to work unless given a lot of unnecessary permissions, mainly microphone and SMS reading permissions.

6.2 Data Usage

a. The OSN should use the data only to show advertisements. It should be clearly mentioned on the post that it is an advertisement. The advertisement should not be disguised as a post from the user's feed.

b. News articles should be filtered only on the filters selected by the user and not on the basis of the data collected as a result of the user's activity.

c. User's activity about political posts and events, or other sensitive social elements like racism or religious ideology should not be saved and / or used to filter news articles.

d. News articles that the user receives in their feed must be completely unbiased.

6.3 Data Sharing

a. The OSNs sharing user data with 3rd party companies should take responsibility of the security of the data. That is, the party sharing the information should verify the details of the company with which they are sharing the information. The minimum requirements that must be fulfilled by the company requesting the information would be set by the Data Protection Audit Board. The data sharing can be done only when the company requesting the data fulfils the said criteria.

b. The 3rd party companies should inform the users regarding the source of data and their intention for using the data for specific use viz. advertisement, research etc.

c. This information should be in form of text message and/or email to the user. There should be 3 messages or email in the period of one week to the user, after which the companies can start sending the target messages or email.

d. Each message should have an 'unsubscribe' option written in bold, with font size of 10 at the bottom of the message/page. Once user unsubscribes for the particular service, user should not receive any further correspondence regarding the same advertisement. However, if the product/object of advertisement has changed, then again an acknowledgement has to be sent as per point {c}.

e. The 3rd party companies sharing user data obtained from another company further with other companies / individuals should also be held liable for user data. Likewise, the entire chain where user information is passed on should be accountable for protection of user data in case of any infringement.

f. User should have right to filter some of the data (opinions about sensitive issues, personal details) that they don't want to share with 3rd party companies.

g. The OSN should audit the usage of the data by the 3rd party companies and make sure there are no violations. The OSN should be held liable for any violations by the 3rd party.

6.4 Data Storage

The OSN should make sure that user's data is stored in a secure manner.

a. The data stored should be in an encrypted format and not in plain text. [12]

b. Security measures should be taken to prevent any unauthorised access to the data.

c. The data should be stored only until the permissions for the data usage are valid. For example, if the OSN (or 3rd party) has right to store data for 6 months, the data should be permanently discarded promptly when permission expires.

6.5 Data Deletion

User data must be deleted if any of the following is true:

a. The stated "purpose" has been accomplished (either successfully or unsuccessfully).

b. The stipulated time period has expired.

c. The user has expressly asked to delete the information.

d. The user should have the right to be forgotten. Right to be forgotten is the right of the user to be removed from any and all databases of the OSNs or 3rd party companies. This right can be invoked in 2 cases:

   i. User deletes their account from the social media website

   ii. User expressly asks the OSN to delete a part of their data from the website.

This information should only be stored in the archives which can be accessed in the case of legal requirements. The data cannot be used by the OSN or 3rd party without the approval from the Data Protection Audit Board (discussed in point number 7).

6.6 Terms and conditions

a. The terms and conditions and privacy policies should be made easier for the users to read and understand. For this:

   i. Permissions can be categorised into various headings, and a short permission sheet should be provided to users which states all permissions that a user has granted the OSN.

   ii. It should also state clearly the permissions that the OSN does not have. For example: We reserve the right to use your photographs for targeted advertisements and sharing them with 3rd parties. However, we do not have permission to modify those photographs.

b. There should be an optional "Read full terms and conditions" option that provides user with an unbridged version of all the terms and conditions.

c. The Data Protection Audit Board should audit that the summary provided by the OSN reflects the true terms and conditions of their agreement.

d. The user should be made to read the terms and conditions whenever signing up or whenever there are a modification in the terms. For this, OSN can take step by keeping the next button disabled until the time it takes to read the summary. The time taken should be at least equal to the time taken for the screen reader to read the summary.

e. The font and the font size of the summary as well as the terms and conditions page should be kept to a standard as decided by the Data Protection Audit Board. (For example, font face: Times New Roman, size: 12, line spacing: normal).

f. The Terms and conditions page should be responsive to the size of the screen and effectively scale down to the size of tablet or mobile devices.

6.7 Data Protection Audit Board

A separate, dedicated board should be set up for dealing with data protection issues on the Social Media websites. This board can work in collaboration with the Ministry of Electronics and Information Technology of Government of India. The board would be a parallel of a consumer forum. It would address all consumer issues faced by the users of the OSN. The duties of this board would include:

a. Defining the term "sensitive data" and whether OSN has right to store them.

b. In case of a legal issue pertaining to a user's data that has been deleted by the user, grant access to the archives of the social media for resolving the matter if the case merits the disclosure of the data.

c. Audit the validity of the Terms and Conditions of the website as well as the summary of the same provided by the OSN.

d. Decide upon the specifications of font type, size, colour, etc. for the Terms and Conditions of the websites.

e. Monitor the websites to ensure there are no violations of the law.

f. Users who feel that their data has been compromised should be able to approach the Data Protection Audit Board. The Board will then launch an investigation into the case.

g. Draw up a set of criteria that a company must pass before it can legally obtain user data from any source.

h. Settle matters of dispute in case of conflict in fulfilment of criteria.

6.8 Punishment for Infringement

a. The Data Protection Audit Board will investigate into allegations of infringement. If found guilty, the Data Protection Audit Board has the right to

   i. Impose a fine on the company that has infringed the rights of the user(s).

   ii. In case where the guilty company is not verified, impose a fine on the company that shared data with the guilty party.

   iii. Impose an operational ban on the guilty website(s) for a certain period.

b. The punishment should increase for each subsequent offence to ascertain that further infringement does not occur.

7. CONCLUSION

Internet and social media websites are an essential part of our lives. People are now interested more in their social life rather than the real one. And to keep their social media profiles updated, they keep adding more and more information on social media websites. This gives social media websites a lot of scope to exploit the data of the users by using them for advertisements as well as other means. We can see from the awareness survey mentioned in the paper, that social media users are easy targets and not much aware about the business tactics of the social media. In such a case, we need strong laws to safeguard the interests of the social media users. The guidelines discussed in the paper, if implemented, can go a long way to regulate the social media environment and help their users use the internet more safely. It will ensure that user data does not get misused by the social media websites and protect the users from the consequences of data leaks mentioned above.

8. REFERENCES

[1] How targeted advertising works - https://www.washingtonpost.com/apps/g/page/business/how-targeted-advertising-works/412/?noredirect=on

[2] Does India have a Data Protection law? - http://www.legalserviceindia.com/article/l406-Does-India-have-a-Data-Protection-law.html

[3] Mafaisu Chewae, Sameer Hayikader, Muhamad Hairulnizam Hasan ,Jamaludin Ibrahim (2015). How much Privacy we still have on Social Network? - International Journal of Scientific and Research Publications.

[4] Graham-Harrison, Emma; Cadwalladr, Carole (March 17, 2018). "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach". the Guardian. Archived from the original on March 18, 2018.

[5] Aadhaar faces yet another data leak allowing access to personal data to "all" enrolled in the system: report https://www.firstpost.com/tech/news-analysis/aadhaar-faces-yet-another-data-leak-allowing-access-to-personal-data-to-all-enrolled-in-the-system-report-4403621.html

[6] Canadian Business Banking Customers Hit With Targeted Phishing, Account Takeover Attacks - https://securityintelligence.com/canadian-business-banking-customers-hit-with-targeted-phishing-account-takeover-attacks/

[7] Indian IT Act 2000 - http://www.dot.gov.in/sites/default/files/itbill2000_0.pdf

[8] Vishalakshi Singh. An Analysis of Personal Data Protection with Special Emphasis on Current Amendments and Privacy Bill - International Journal of Law and Legal Jurisprudence Studies

[9] The Personal Data Protection Bill - https://cis-india.org/internet-governance/blog/the-personal-data-protection-bill-2013

[10] Shadow profiles are the biggest flaw in Facebook's privacy- https://www.theverge.com/2018/4/11/17225482/facebook-shadow-profiles-zuckerberg-congress-data-privacy

[11] Google Has Been Hearing You With the Help of Your Phone's Mic - https://www.thequint.com/tech-and-auto/tech-news/google-record-phone-conversations-save-them-on-website-users-can-delete-them-dont-use-google-voice-search

[12] Twitter Corrected a Bug That Caused Passwords to Be Stored in Plain Text - https://www.adweek.com/digital/twitter-corrected-a-bug-that-caused-passwords-to-be-stored-in-plain-text/