International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 05 Issue: 02 | Feb - 2021 ISSN: 2582-3930

Data Privacy Concerns in Social Media

Minakshi Khatri, Piyush Wasalwar, Shruti Sharma, Sindhuja Shankar

Minakshi Khatri, Marketing Management, MIT WPU

Piyush Wasalwar, Marketing Management, MIT WPU

Shruti Sharma, Marketing Management, MIT WPU

Sindhuja Shankar, Marketing Management, MIT WPU

Mark Zuckerberg, the founder of Facebook, states, *"I wanted to create an environment where people could share whatever information they wanted, but also have control over whom they shared that information with"* (Zuckerberg, 2006, para. 3)

❖ **Abstract:**

As most use the internet essentially for exchange, many use it for academic purposes, while others use it for other purpose as communication and sharing data, many of them use for entertainment purpose. Therefore, the internet can be compared to a blank check, which serves various purposes as of how one individual use it and make it useful for own purpose, and how an individual wants it to be described. In view of the internet's consumer diversity, recent studies have actually done shows an element of internet usage that appears to have caught up with over 70% of all internet users has been verified.

This research paper was carried out with the intention of defining the privacy concern related to the use of social networking sites and social media networking activities. For this the questionnaire was prepared for 250 participants for people. The people who responded were from different background and different education qualifications. The primary source of data was about the attitude of respondents towards privacy concerns was primarily emphasized when using social networking sites. The primary exercise in data collection was also committed to understanding the depth of information about privacy issues with networks for social media and how people react to it.

❖ **Keywords:**

Data privacy, relevant ads, Social media, Social media marketing, Social media networks

❖ Introduction:

Communicating with each other is quite easy in today's world with new technology and equipment. Apart from phone calls, and text messages, Social media is a highly effective tool to communicate with each other. You can share all the relevant information and get the information with one click, apart from that without saying a word you can convey your feelings and emotions through pictures and writing. In the same way, you can read and, are in a position to analyze people's feelings and thoughts with the picture they share and words they write. This is the new way to communicate. Each person sharing and communicating with the world through a different platform and media gives rise to huge amounts of data. Data is defined as an interpretable representation of information in formalize manner suitable for communication, interpretation, or processing. (Minnesota, 2021). As there is a lot of data available around, it is very easy for people to analyze and predict the preferences of people. With help of posts and pictures that people share, knowing their preferences and choices they make is easily judged. Commenting on the picture and liking a particular product gives an insight into their liking and gives the advantage to expose themselves in front of the world. The privacy of the individual is not in one's hand with this. The privacy of his data is a big thing to deal with.

Data privacy, sometimes also referred to as information privacy, is an area of data protection that concerns the proper handling of sensitive data including, notably, personal databut also other confidential data, such as certain financial data and intellectual property data, to meet regulatory requirements as well as protecting the confidentiality and immutability of the data(S, 2021) Various companies use public data to place their ads and brand themselves using social media. Seeing the preferences and liking of a picture of the product, collected from this data, coming across various ads and recommendations is not a new thing in social media. This type of strategy by collecting data and using it to market and keep track of people is done by the social media company and the various companies which are interested in people preferences and choices so that they can reach the target audiences with more efficiency. In a way, there are various risks associated with this type of data for people and times are manipulating the preferences and choices can be done through the same.

This paper is about people's choices and their preferences regarding data privacy. The various risks associated with using social media and how aware the people are regarding their privacy on social media. What is their take on this type of practice and their choices of preferences over data privacy?

❖ Statement of Problems:

Sharing on popular social networking sites has become a trend nowadays, people feel comfortable about sharing their private life online but the problem here is not sharing your data online but concerning about privacy. A case study shows that users of social networking sites such as Facebook, Instagram, Twitter have now become more open and

sharing more and more personal information online with number of people. In these modern times this may have become a trend, but users should be aware about the information which they share online can be used in harmful ways such as for stalking or identity theft. Therefore, a balance should be maintained between online disclosures of personal information and privacy as the scales increasing maybe harmful to the users.(Minfest, 2019)

In recent years, these social networking sites have attracted millions of people as on such sites people can share and communicate with anyone sitting in any part of the world. These sites allow users to create personal blog or page that represents their social connects, easily share media content and share the daily updates of their life with friends and family online. However, there are potential threats that are related to user's privacy, as personal information is exposed on internet to wider audience and often information about a user are posted by others maybe by friends, colleague or family without his or her consent and this produces a major risk of leaking personal identity and information. Therefore, its important that social media sets some boundaries of what personal information are to be provided to the public. Such threats can be personal identity theft, Stalking, sexual predators, online victimization, location updates etc.

From a social media privacy perspective, the study gives us some very concerning results. It turns out as Social media team didn't even need 10 accounts to figure out a person's profile. They just need to see some tweets and Facebook uploads and they can start creating some startlingly accurate profiles. For example, machine learning algorithms which are popularly used as for giving you accurate predictions start to figure out person's profile by considering some factors like "political affiliation" or "leisure interests" simply by studying the tweets of someone's friends. Often, their results are proven to be 95 percent accurate. If a person is no longer on any social media sites, they are still able to figure out details by friends or colleagues who all are active on such sites. The study is an affirmation of the adage, "Tell me who your friends are, and I'll tell you who you are". Even if a person decides to delete a social media account, his profile is still "encoded" in previous activities with his friends such profiles are called as "Shadow profiles of non-users". Thus, one can think that your friends are creating "mirror image" of yourself.

This site obviously has social media privacy implications. In a base case scenario, some brands are able to craft marketing messages customized for such users, simply by analyzing the stuff you share online in your network. Search engines are able to deliver search results which fits to specific people based on what their friends are saying. And even in worst case scenario, an authoritarian government might be able to figure out group of political dissidents quickly by applying few machine learning algorithms. They can also manipulate your voting decision by showing you wrong perception of your leaders and it might be possible to change a person's mind by fulfilling their needs and wants without even suspecting, solely on the basis of Internet users on social media.(Lindsey, 2019)

There's another element to the research is that social media privacy is not necessarily an individual's choice. Friends can share personal information about you on social media, even if a person is doing everything to protect social media privacy (deleting account or restricting access to personal data) still data is collected. Users of social media accounts are in control and their activities are also been recording without informing them.

❖ **Need for Study:**

Social media today is a very vast term, consisting of Facebook, Instagram, Snapchat, WhatsApp, etc. It is gaining more and more popularity with each passing day and the number of users on such platforms is ever increasing. The prime focus of this research paper is to get an idea of the awareness of privacy policies of various social media problems. It also gives us an insight of people's perspective on data privacy on social media and helps us find out if the users are comfortable with their data being used in the process of providing them with ads relevant to their preferences.

❖ **Literature Review:**

The last decade has witnessed a rapid growth in the number of individuals using Social Networking Sites (SNSs). Although SNSs provide many benefits for individuals such as keeping in touch with friends and family, privacy and security is regarded as a critical issue that can threaten the users of SNSs (J, 2007). This is mainly because SNSs encourage their users to reveal a great deal of personal information about themselves by promising them a better user experience if they do so (Li, 2015) When users first sign up to Facebook, they will be constantly asked and reminded by Facebook to update their profile with more personal information such as date of birth, hometown, workplace, and/or school in order to find more friends and enjoy the experience more (Lewis, 2015) Threats from SNSs can be divided into two different categories - security and privacy.

These terms sometimes overlap and may be used interchangeably by users and researchers. Therefore, in order to provide a clearer conceptualization, the key terms, privacy and security, will be defined as follows with respect to SNSs:

Security: In SNSs, security threats result from the technical vulnerabilities of the network (Altshuler, 2015) In 2009, the Secure Enterprise 2.0 Forum identified and listed eight main security threats that may occur when using social networks (Chi, 2011): insufficient authentication controls; cross-site scripting; cross-site request forgery; phishing; information leakage; injection flaws; information integrity; and insufficientanti-automation.

Privacy:The increased use of information and communication technologies has had a significant impact on the interactions between users. This is particularly true for people who use mobile devices to communicate with one another or to access the Internet. Mobile web users have difficulty knowing where and how their information is stored

and who is authorized to use it. Therefore, protecting mobile user internet knowledge and increasing their confidence in knowledge privacy has been a true challenge. (CAVOUKIAN, 2009)Coined the term "privacy by design" which refers to the need to address privacy concerns from the outset. The author outlined it as a philosophy to boost style by embedding privacy issues as needs into areas of style like technology style, business practices and physical style. The "privacy by design" issue has become the most basis of on-line application styles. totally different social network suppliers like Facebook, Google and Twitter area unit competitor to produce tier of privacy in their applications that will inspire confidence in their users.Using the concept "privacy by design" as a standard for designing applications will give users more authority to decide what kind of information they want to share with whom. (Nahier Aldhafferi, 2013)

Social network and privacy:Social network and privacy Technology has influenced the society in amazing and innovative ways. Social networking is one of the greatest influences in the 21st century. Up to 1.4 billion people are using various social networking sites to communicate in real time, share photos and videos. (B, 2013). Use of social networking has grown to include all people of all ages including the very young, the young, the mid aged and the old. Politicians around the world have also taken advantage of the benefits of the social networks to communicate with their followers. While the use of social networks has grown remarkably, the privacy and safety of the user's information concerns have also increased. Many people wonder whether there are people who have access to the details they provide. The hacking of some of the social networking websites has also raised a lot of privacy concerns. Social networks have availed instant communication and sharing but there are grave concerns about privacy, which should be addressed to allow more people to experience the advantages of the new technology. (Salerno J, 2011)

Online privacy risks:There are several risks surrounding the posting of personal information details on social networks. These threats can be caused by hackers or spammers who obtain users' personal information details. Identity theft is one of the major risks that users face (WILLIAMS, 2009). Access to sensitive information may also lead to terrorism risks, financial risks and physical or sexual extortion (GHARIBI, 2012).

(GAO, 2011)Mentioned the common privacy breach attacks in on-line social networks. First, users sometimes transfer their personal data once they trust the service supplier. However, the provider can use these details for business functions like advertising. Additionally, it's not solely the service suppliers UN agency will see the users' personal data. Some on-line social networks supply users with policies to examine the list of commissioned person international organization agency can see their personal information. These policies vary from one provider to another; some suppliers offer users heaps of flexibility than others and many supply secret writing for his or her data.. The second privacy breach will be caused by the user's friends, UN agency will share the user's personal data details with others. Friends UN agency have access to the user's personal data will copy and publish this data. The third breach is because of spammers. once spammers see the user's friend list, they will see different users' personal data by causing them an

exponent request, impersonating one in every of his/her friends by victimization the friend's name or image. Lastly, breaches will be caused by third party applications put in by users. These applications will be a threat to users, particularly if they're not from a trusty supplier. once the applying accesses the users' personal data, others will acquire this data.

(NOVAK, 2012)Also, claimed that privacy breaches can be caused by friends, applications, and exploitation of personal information details by the service providers for advertising. The authors added that understanding privacy settings is not enough to protect users, especially from friends and other online social network users. Thus, social networking websites such as Facebook prioritize the development of tools to protect privacy. This is manifested in the social network providers' requests for new users to create new privacy settings. However, some users do not realize the risk of leakage of personal information (LEE, 2011) Therefore, sensitive information such as home address and date of birth should not be posted on the internet in order to be safe from privacy breach. Increasing user awareness of these risks, providing a privacy management system for users to control their personal information details, and constantly updating privacy policies can lead to a decline of these risks (GHARIBI, 2012).

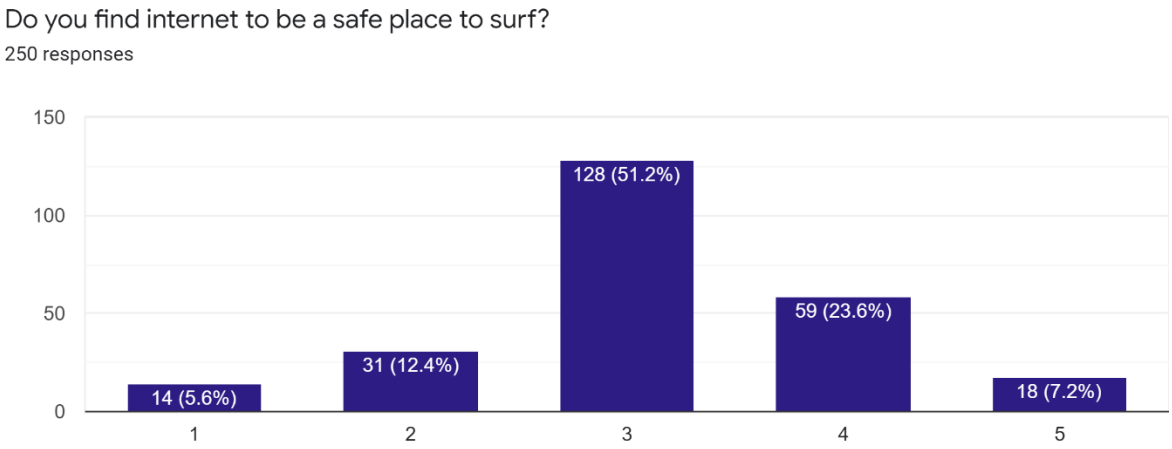
❖ Research Methodology:

This research is conducted with the help of both, primary and secondary data. The primary data was collected using a questionnaire consisting 10 questions on the lines of data privacy, convenience of getting relevant ads and if this use of personal data was a topic of concern among the sample targets. We framed a Google form and circulated it amongst family, friends and colleagues. With the help of this form, we could get inputs of 250 people of different age groups and gender, which gave us a diverse sample. Along with this, we have also referred to research papers for our literature review to get a more in-depth knowledge regarding the same.

❖ Data Analysis:

To do a further detailed study we sent across a questionnaire targeting all age groups, that helped us gain an overall view of the opinions of people on data privacy and their willingness to trade their data for convenience.

We started with a question asking how safe people found the internet. The response to the same can be graphically represented as follows:

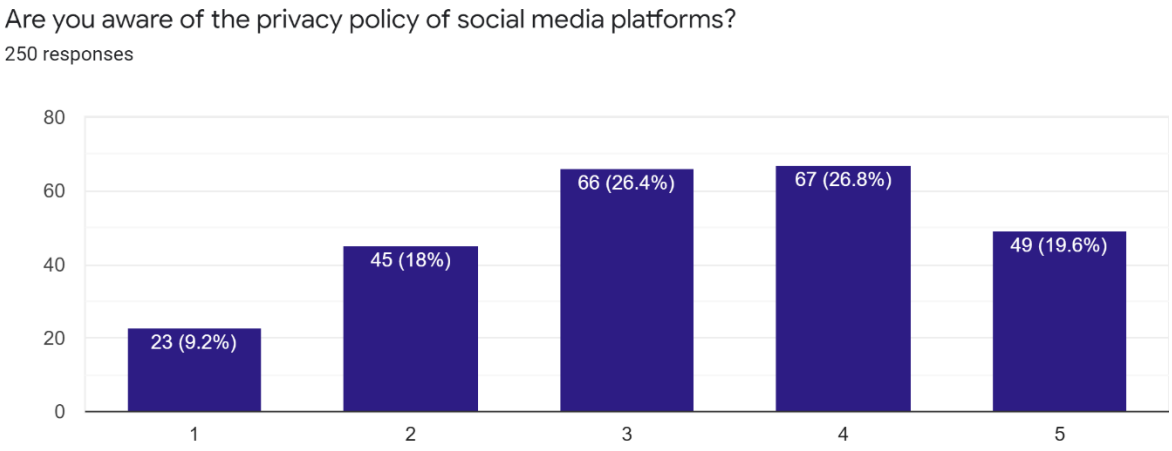


We see that majority people are unaffiliated to the major extremes and prefer to go ahead with a neutral opinion. However, it is also clear from the graph, of the remaining, majority find internet to be a safe place to surf.

To further bifurcate on the basis of age, it was observed that:

- Children and teenagers, of age 11-20 on an average find internet a safe place to surf.
- Youth, belonging to the age group of 21-30 seem to be scattered but majority can be seen to having a neutral opinion.
- Tricenarians, belonging to the age group of 31-40 find Internet on an average a safe place to surf.
- Likewise, taking an average of age group 41-70 people have a neutral opinion about surfing on Internet.

In order to know the basis on which people commented on if they find internet to be a safe place, we further went on and asked them to rate their awareness of the social media privacy policies, the responses to which were:

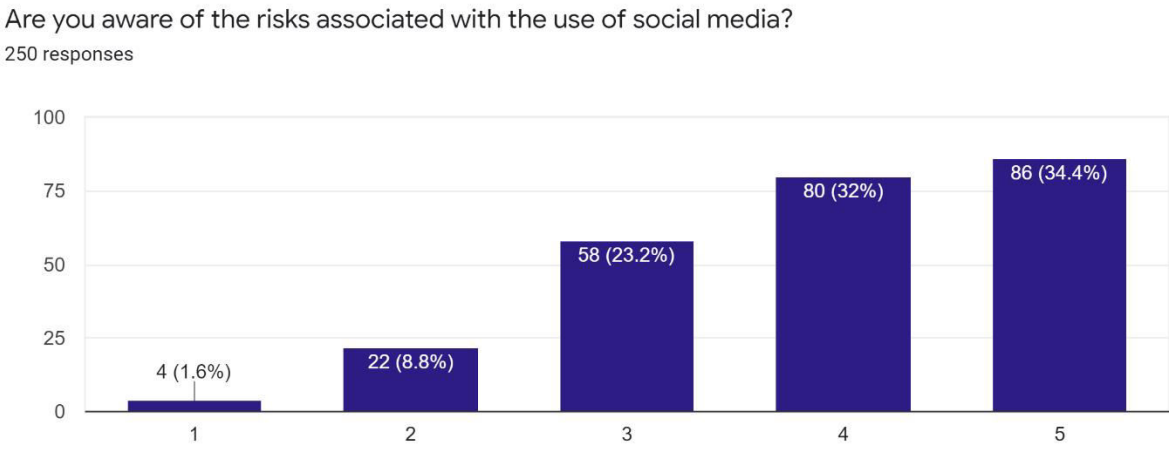


With the graph above, it can be interpreted that majority of the people believe that they are well aware of the privacy policies of social media which can assumed to be because of the recent change of privacy policies of WhatsApp.

When we bifurcate the above data on the basis of the different age groups, it was noticed that:

- Children today seem to believe that they are aware of the privacy policies of social media today. Even if that is not the case, they are at least not ignorant of a term like “privacy policy”.
- Talking of today’s youth, roughly 80% of the youth who answered our questions seem to be aware of the privacy policies, while the rest 20% seem to be comparatively unaware of the same.
- Further considering age group of 31-40, 40% people are slightly aware about the privacy policies and whereas 60% people are not much aware about the policies.
- Quadragenarian and above age people appeared to be not aware about the privacy policy of social media platforms and only 30% of them are bit aware of the same.

Further, we moved on and asked people how aware they were of the risks associated with the usage of social media, keeping in mind the privacy policies regarding data as discussed in the earlier question. The responses for the same were:

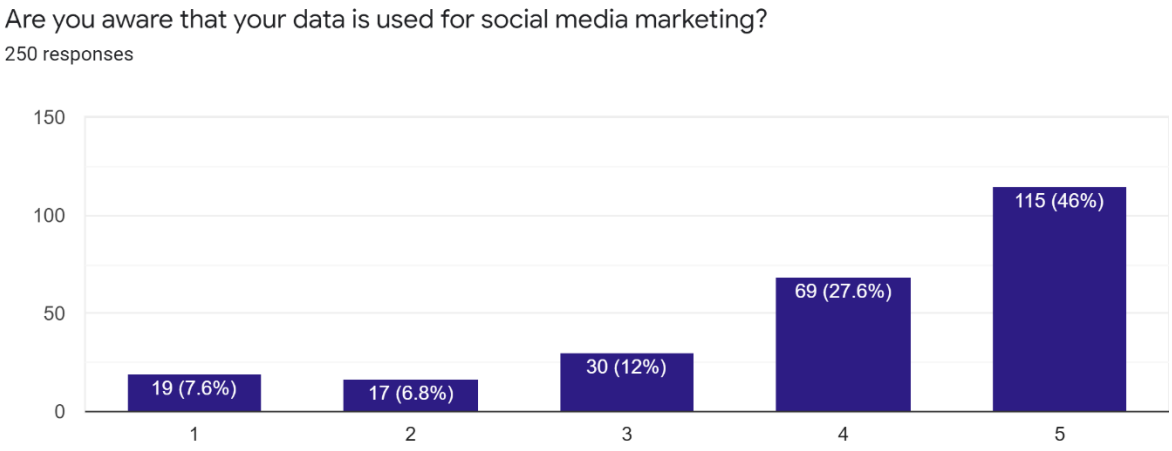


With roughly 66% of the audience stating that they are well aware of the risks, it can be interpreted that even people who stated that they were unaware of the privacy policies are aware of the same when it comes to risks that one faces while using social media.

The same, when compared on the basis of age, shows that:

- Children of age group of 11-20 seemed to be well aware of the risks associated with social media. Furthermore, in a sample space of 14 responses, there were 11 girls and all of them had responded stating they are acquainted with the risks.
- However, surprisingly, the youth had a few responses that showed that there was a part of the audience that was not aware of the risks, while majority seemed to be well aware.
- People among age group 31-40 and 51-70 are bit familiar with the risks associated in using social media while age group of 41-50 on an average have neutral responses about the same.

Moving closer to the main focus of this research, we then asked people if they were aware of the fact that their data is being used for social media marketing (SMM), for which the responses can be summarized as:



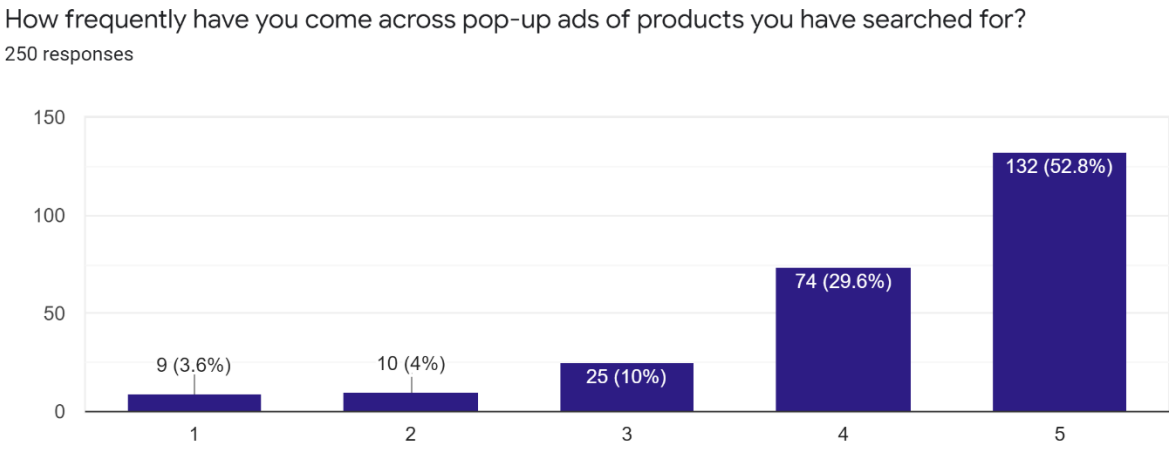
It can be clearly observed that around three-fourth of the target audience are aware that social media marketing requires usage of their data. This part of the questionnaire can said to be in alignment with the data regarding the awareness of the privacy policies of social media, where, if one is unaware of the privacy policies, chances of the person being well-versed with the functioning of SMM might be comparatively low as well.

The age wise responses for the same were:

- 80% of the audience, belonging to age 11-20 say that they are well aware of the functioning of SMM
- Similar to the responses of the children and teenage category, majority of the youth too is aware that their data is being used for SMM.
- Tricenarians seemed to be aware about the use of their data for SMM while 85% of the people who belongs to age group 41-50 are partially aware that how their data is being used for SMM.
- Similarly, with people in the age group of 51-70, it has been observed that they are much aware about the usage of data for SMM.

We then shifted our focal point towards the personal experiences of the audience by asking them if they could observe a relationship between their search history and of what they speak, with the pop-up ads that they come across, the responses to which were:

A) Using their search history:

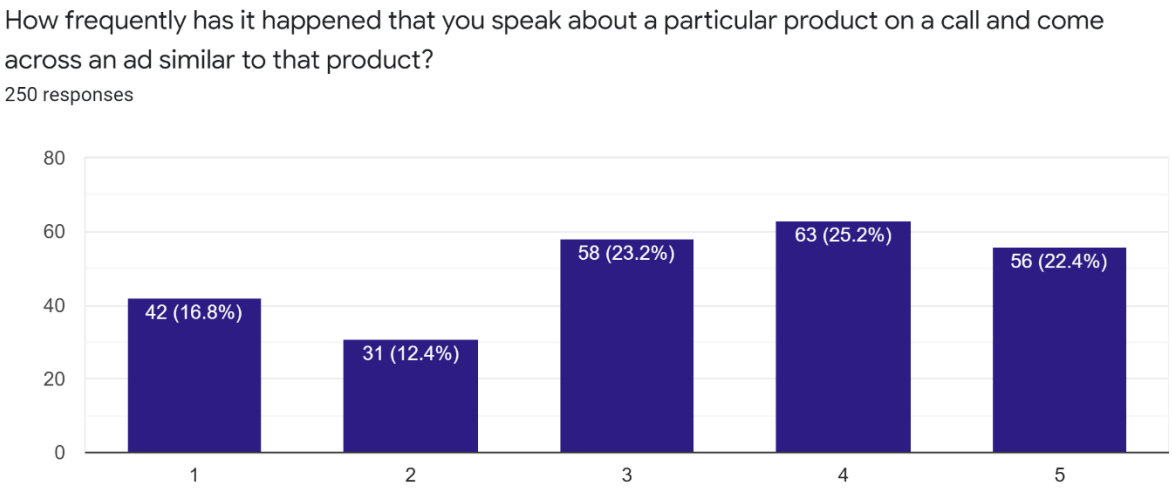


80% of the sample say they come across pop-up ads related to their searched for, while the remaining do not come across the same that frequently.

Taking in consideration the age of the sample:

- Almost all children and teenagers of the sample audience said that they come across such pop-up ads very frequently.
- Here too, a major chunk of this age group, about 95% of them, said that the frequency of these pop-up ads was on the higher side.
- Individuals with age 31 and above experience pop-up ads after their search on social networking sites amongst which 10% of them does not come across with the same experience.

B) With the help of the access to their mic:

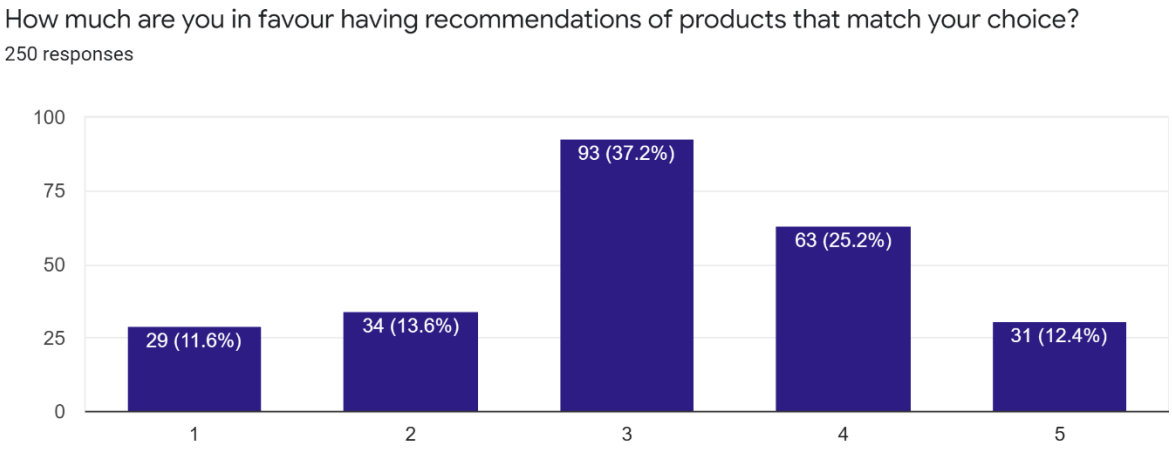


The responses for this question are scattered. Here we have a good mix of people who have rarely come across such related ads as well as those who come across such ads much more frequently.

To further bifurcate on the basis of age, it was observed that:

- Children and teenagers have not come across ads related to products they have talked about when their mic was on.
- While as opposed to children, the youth have come across ads related to products that they have previously mentioned with their mic on.
- Majority of people, belonging to age 31-40 frequently come across with such related ads which they speak about on call and same happened with the age group of 51-70.
- Whereas mid-aged people do not experience with the same issues as the other age group. They do not come across with such related ads on their social networking sites.

Assuming that the ads based on people's search history and on the keywords that they use when they have their mic on will be relevant to them, we further went on with the question where we asked the audience how much they are in favor of getting such relevant ads. The graph below shows the same:



They have neutral approach towards having recommendations for their product. The audience majorly wants these recommendations but not a lot. This could be because getting constant ads could be irritating for the audience.

The same, when compared on the basis of age, shows that:

- Children and teenagers are considerable not very much in favour of having recommendations for the product that match their choices and demands.
- Comparatively, we can say the youth are more interested in having these recommendations, but however the numbers are not very promising.
- Almost every individual within the age group of 31-40 have neutral opinion about having recommendation of their matched product.
- Contradicting to above statement, 41-50 aged group people are not much in favour of having recommendation about their preferred product choices.
- And matching with the elder group people till 70, 60% like having recommendation of their searched product or services, and 40% are in neutral opinion.

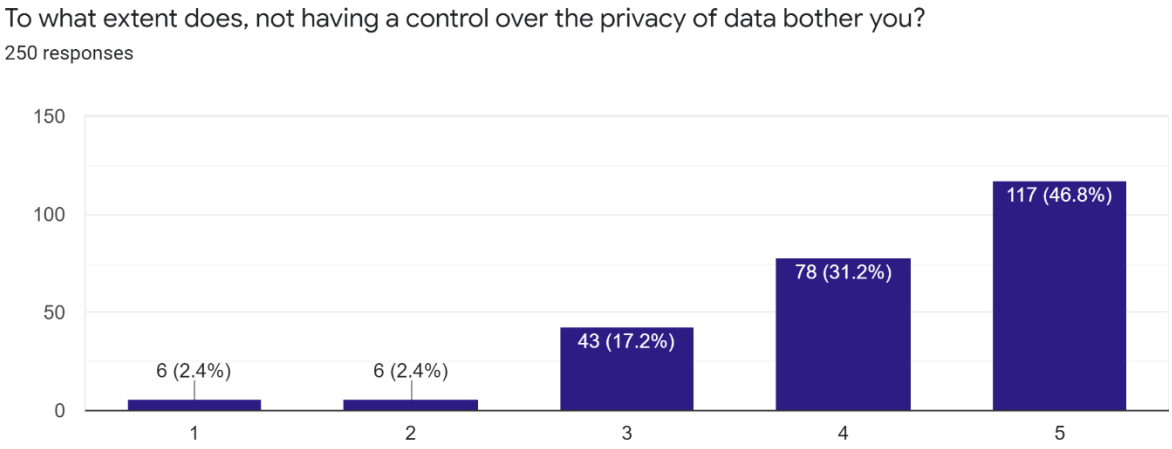
And to further focus on the prior question, we asked the audience to choose between data privacy and getting relevant ads. The following pie chart shows the same:

We see that even though the responses of people were more in the favour of relevant ads in the previous question, when given a choice between data privacy and getting relevant ads, majority of them prioritize data privacy. They tend to give more importance to data privacy than to convenience in shopping.

Taking in consideration the age of the sample:

- In the first group, the responses showed the preferences of audience to be equally divided. There were almost equal votes for both the parameters.
- In the second group, we witnessed that around 80% of our audience is choosing data privacy over relevant ads.
- Data privacy is the main concern of most of the people in the age group 31 and above and only minority (5%) give preference to relevant ads.

With reference to the question above, we then included a question asking people to rate how bothered they were with the low amount of control that they have on the privacy of their data. The responses can be graphically summarized as:



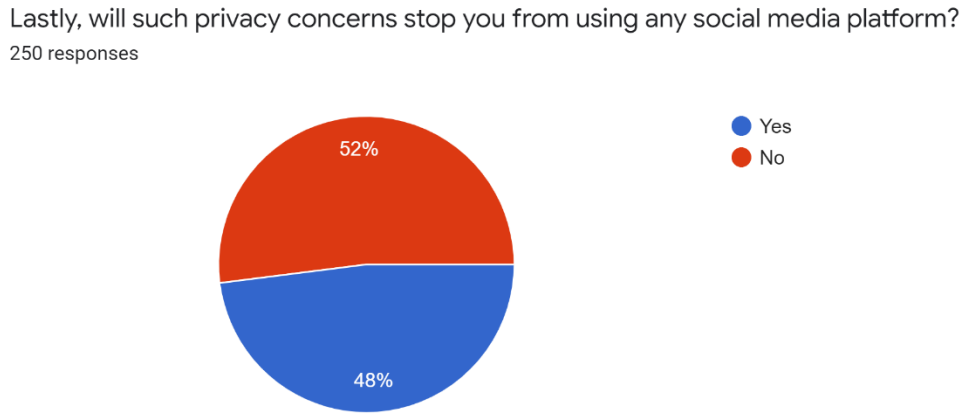
With the above data we can interpret that more than 70% of our audience are bothered with not having control over the privacy of their data. Although there are around 17% people who seem to be indifferent about the same.

The same, when compared on the basis of age, shows that:

- It is pleasant to know that children and teenagers are concerned about having control over the privacy of their data. We can also interpret that they seem to be aware of the shortcomings of their data not being private.

- Between the age of 21-30, amongst 129, a mere 6 of them are not bothered, while 24 of them seem to care less of their data privacy.
- Almost everyone of age group 31-40 and 41-50 from our collected find it inconvenient of not having control over their privacy on social media.
- Whereas elder age group people with 50 and above seemed like they are highly bothered with the concern of not having control over privacy of data.

Moving on from the level of concern our audience had over the control they had over their data privacy, we went on to ask them if they were willing to switch from the social media platforms, they are currently active on to other social media platforms that offered more privacy of their data. The results of the same are:



It is crystal clear from the pie-chart above that our audience was more or less equally divided when it came to this question. While 48% of our audience said they were willing to switch, 52% preferred to continue with the ones they are currently using.

The age wise responses for the same were:

- In the 11-20 age group, 70% of our audience preferred not to switch over to other apps.
- While the part of audience belonging to age 21-30 seemed to have been more or less equally divided, with majority of them not willing to shift to any other platform.
- Analysing the data, there were neutral preferences for the age group of 31-40 when asked if they were willing to shift.
- Given the choices, to age group 41-50, they are more likely to shift to new social media platforms.

- And opposite to this, people with age group 51-70 are ready to give up on the usage of the social media platform they are currently active on.

❖ **Challenges/Limitations/Shortfalls**:

a. Geographic restrictions: The major obstacle while doing our research was that of the geographical restrictions. Our data is restricted to the audience of the state of Maharashtra and hence is a very thin slice out of the big fat cake. This data is centred only to the cultures and believes in one state of India. We have not focussed on the mind-set, cultures and believes in other Asian countries, European countries and the US. People belonging to different parts of the country, and world, might have different views. This is because the views of people are characterized by their cultural backgrounds which is in turn influenced by the place of residence. So focusing on people from just one state does not give a clear idea of the overall view on the topics.

b. Subjective scales: The perception of privacy, security is differs from person to person and does not have a standardised benchmark to judge from. We thus inferred that what might be safe for one may not be safe for the other. Without a proper benchmark it was tough for us to interpret, process and analyse the data.

c. Narrow scope of research: The focus of this research paper is solely inclined towards the data privacy preferences of people with regards to social media marketing . We did not penetrate further into the issues arising within the umbrella of data privacy and security such as Identity theft, Hacking, Shadow profiling, Cat fishing. While doing our literature review we hence had less data to read and understand from.

d. Insufficient sample size: The data collected by way of primary data cannot represent the whole population, as our sample audience consisted of a mere 250 people, which is a negligible part of the whole population.

e. Limited access to data: The changes in the privacy are so often that keeping up with them can be a task. Because of this dynamic characteristic of data privacy we can say that the data today might be outdated tomorrow.

❖ **Conclusion**:

To summarise our findings, we can say that our audience are well aware of the privacy policies and the risk involved while surfing on social media, but yet find it a safe place to surf. This shows that the risk doesn't bother them maybe because of the knowledge of the topic. Further we also see that the audience are bothered by the data privacy concerns, but it does not stop them from being an active social media user. The audience does have a concern regarding data privacy but yet do not want to shift from these applications. This could be because they might be unaware of the options available or habituated to the ones they are using. The age group of 31 and above are concerned with the control over their data privacy because in the earlier responses we realised that they were not aware of the privacy policies of these social media applications. The unawareness of these policies could be one of the reasons for their hesitance while using social media. We thus conclude that major part of our sample is bothered by the data privacy policies, but still continue with these social media sites. Some are comfortable with their data being used for social media marketing while some or not. Companies need to take in mind the preferances of the users and use their data. In all, we witness that even though our audience seemed to state that data privacy was their priority and they were not willing to let their data to be used, the end results were more or less balanced. Hence, we can say that the facilities provided by social media somehow tend to overshadow the risks and issues it comes with.

❖ **References (APA Style):**

- J, D. (2007). Signals in social Supernets. *Journal of Computer-Mediated Communication, 13*(1), 231-251.
- B, A. N.-J. (2016). Social Network and Privacy. *Journal of Mass Communication and Journalism, 6*(1), 1-8. Retrieved from https://www.hilarispublisher.com/open-access/social-network-and-privacy-2165-7912-1000288.pdf
- B, A.-J. (2013). Satisfying public Relations: The promise of Social Media. *International Journal of E-Adoption, 5*, 1-16.
- CAVOUKIAN, A. (2009). Privacy by design…Take the Challenge. *Information and Privacy*, 6.
- GAO, H. H. (2011, JULY). Security Issues in Online Social. *Security Issues in Online Social, 15*(4), 56.
- GHARIBI, W. &. (2012). *"Cyber threats in social networking websites.*

- LEE, R. N. (2011). "Design and Implementation of FAITH, An Experimental System to Intercept and Manipulate Online Social Informatic. " *Advances in Social Networks Analysis and Mining (ASONAM).195*, p. 202. Advances in Social Networks Analysis and Mining (ASONAM).
- Nahier Aldhafferi, C. W. (2013). PERSONAL INFORMATION PRIVACY SETTINGS OF SOCIAL MEDIA. *International Journal of Security, Privacy and Trust Management, 2*(2), 1-17. Retrieved from https://arxiv.org/ftp/arxiv/papers/1305/1305.2770.pdf
- NOVAK, E. &. (2012). *A Survey of Security and Privacy in Online Social Networks.* College of William and Mary Computer Science Technical Report.
- Salerno J, Y. S. (2011). Social Computing, Bheavioral Cultural Modeling and Prediction. *4th International Conference.* USA.
- WILLIAMS, K. B. (2009). "Social Networking Privacy Behaviors and Risks. *Seidenberg School of CSIS, Pace University*.
- Minnesota, U. (2021). *Libraries*. Retrieved from Minnesota University: https://www.lib.umn.edu/datamanagement/whatdata
- S, O. (2021). *SNIA*. Retrieved from What is data privacy?: https://www.snia.org/education/what-is-data-privacy
- Lindsey, N. (2019, March 12). *CPO Magazine*. Retrieved from New Research Study Shows That Social Media Privacy Might Not Be Possible: https://www.cpomagazine.com/data-privacy/new-research-study-shows-that-social-media-privacy-might-not-be-possible/
- Minfest, T. (2019, March). *Data Privacy Concerns: An Overview for 2019*. Retrieved from https://medium.com/@the_manifest/data-privacy-concerns-an-overview-for-2019-2ccea79aa6f8