SAFER-I

Deconstructing Online Privacy: Online User Engagement and Privacy Concerns on Social Media

NEPAL

A Report by
SAFER-I

Jan 2023

Deconstructing Online Privacy:
Online User Engagement and Privacy Concerns on Social Media

Authors:
Nirisha Manandhar, Suvechhaya Shrestha, Aayesha Shrestha, Samyoga Bhattarai

Consultant/Editor:
Ojaswee Bhattarai

Contributors:
Sonika Baniya, Sushobhan Chimoriya

Designs:
Sushobhan Chimoriya, Nirisha Manandhar

Published by Safer-I Nepal

Women Leaders in Technology

2023

Website

Facebook | Instagram | LinkedIn | TikTok | Twitter

Contents

Figures

Tables

Abbreviations

DPC: Data Protection Commission

ToC: Terms and Conditions

SNS: Social Networking Sites

Acknowledgments

This report and the research behind it would not have been complete without the utmost dedication and support of everyone involved in the design, outreach, analysis, and compilation of the findings. We would like to express our gratitude to everyone who took their time and energy in filling out the survey to help us gather different perspectives. We are also grateful to every staff member, alumni, or anyone and everyone else who helped circulated the forms in their circle which helped us reach out to a more diverse pool of people.

We would like to thank Sonika Baniya, Sarila Ngakhusi, and Nasla Joshi for their support during the data collection and annotation phase. We would also like to thank Ojaswee Bhattarai for iteratively guiding us through the research and Sushobhan Chimoriya for proofreading citations and helping with the final compilation of the report.

This report has been published with the support of Open Society Foundations. The views and recommendations expressed in this book are that of Women Leaders in Technology Nepal and do not necessarily reflect the official opinion of Open Society Foundations.

Nirisha Manandhar

Abstract

Social media platforms have been a popular medium for people to pour in their thoughts, get information, and also get connected with friends and families. With this popularity, social media platforms also bring the concern of online data privacy, consent, and data collection. This paper explains how social media evolved and how privacy concerns rose with the increase in social media usage. The main objective of this paper is to analyze the understanding among Nepalese youths of the 18-29 age group regarding data privacy, consent, and data collection by third parties in social media. Our approach for this research is to conduct a survey among youths of Nepal, determine what attributes and factors our targeted population think impacts their privacy and data collection in the social networking sites they use, and visualize those in the form of charts and bar graphs.

Introduction

In today's world, it is rare to come across a young person who does not have a social media account. Social networking sites (hereinafter 'SNS') have become an integral part of how people communicate with each other, with platforms like Facebook, Twitter, and Instagram connecting people around the world and serving as vital communication tools. Recent data shows that 4.74 billion of the total world population are currently active on social media (Kemp, 2022). The same data revealed that until January 2022, around 13.7 million active social media users in Nepal were reported geographically (Kemp, 2022).

The term "social media" as a lay term has a very wide meaning and tends to include a variety of platforms within its scope, mostly used to refer to the frequently and commonly used social networking apps (Kaplan & Haenlein, 2010). Appel et. al defines it as "a group of software-based digital technologies that give users access to digital environments where they can send and receive digital content or information across an online social network, typically displayed as applications and websites" (Appel et al., 2020). Facebook, Twitter, and Instagram are some common examples that fit the definition. Each user defines their virtual borders of online interaction on SNS. These activities can be categorized as:

(1) digitally communicating and socializing with known others, such as family and friends,
(2) doing the same but with unknown others who share common interests, and
(3) accessing and contributing to digital content such as news, gossip, and user-generated product reviews (Lamberton & Stephan, 2016).

People use SNS for a wide range of activities. Be it in terms of forming virtual groups, uploading and experimenting with different forms of media content online, switching to online shopping and

businesses, or even mindlessly scrolling as inactive ghost users, people have taken SNS as a part of their lives - or even more so, it has become a way of life.

Privacy on SNS and attributes that affect privacy practices online

In the age of SNS, privacy on these platforms is a commonly associated topic. The term privacy - as simple as it sounds - might mean different things to different people. An individual might not object to Google collecting their personal information, but could be wary of working in an environment with surveillance cameras. A person could be exceedingly protective of their medical information but quite casual with updating their daily activities in SNS. Depending on the time, industry, and context, ideas of privacy may vary from person to person and it is entirely personal. It is subjective to individual perspectives and contextual to situations. Privacy, as defined in the dictionary by Oxford Languages, is understood as a state in which one is not observed or disturbed by other people. A step further, Westin defines privacy as "the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (Westin, 1968). In today's context where the discussion on privacy is largely concentrated around digital spaces, the definition has been expanded to address these nuances. The Offensive Internet book dissects privacy into four different concepts in light of these contexts. Privacy from one angle could be **valuing seclusion**, meaning the right to be beyond the gaze of others. Secondly, it could be viewed in light of the **level of intimacy** in which one chooses with whom to share certain information. It also may lead to a **level of secrecy** - the act of hiding information from the gaze of others. As for others, privacy might mean **autonomy** in the choices they make (Levmore & Nussbaum, 2012). The need for privacy thus varies depending on different situations. Hence, privacy in the current age should ideally be a flexible and dynamic process where users should be able to control access to information about themselves by managing whom they interact with on SNS (Altman, 1975).

Maintaining privacy is an option available in a variety of dimensions on SNS. Making one's social profile visible could mean **valuing seclusion**. Restricting interactions with one's visible profile could mean **one's level of intimacy**. Similarly, choosing not to disclose one's real identity and personal information like name and location on user profiles could mean **practicing secrecy**. According to Xinru P. et al. in the book 'Social Media and Privacy', achieving the right level of privacy on social media involves negotiating how much, how little, or when we desire to interact with others, along with the types of information we choose to share with them or allow them to share about us. Experimenting with multiple privacy controls and viewer settings lets one decide the level of intimacy with different user groups on these SNS. Many factors affect privacy decision-making, including personal attitudes and personal preferences like gender and sexuality, knowledge of risks and protection, trust in other parties, faith in the ability to protect the information, and monetary considerations (Acquisti, A., & Grossklags, J., 2005). Users' privacy decisions are influenced by a variety of factors, including their participation in risky and careless

online activities without regard for their online privacy, their denial that security threats and privacy violations could pose issues, and their lack of concern for potential privacy and security threats without the need to alter their online behavior (Bubas et al., 2008). In the light of maintaining privacy on SNS, Rodrigues in one of the essays in The Offensive Internet book states how the lack of anonymity options on SNS is a reason why these privacy-enhancing social norms develop online (Rodriguez, 2012). Hence, dissecting the relationship between different attributes and the level of privacy on SNS can be useful in finding out core reasons for such privacy-enhancing behaviors online.

Relationship between the level of privacy concern and the amount of information disclosed on SNS

An interesting approach to viewing privacy online surrounds one's understanding of audience visibility preferences. What does it mean to "publicly" post something? During Mark Zuckerberg's testimony before the House of Representatives regarding the breach of trust between Facebook and its users, the company's executives were seen repeatedly mentioning how they only allow the sharing of data that users have themselves made public (Vincent, 2020). But does publicly sharing mean being limitlessly shareable without consent? When it comes to breaking down cases of the "viral" spread of content in SNS, one might argue that publicly posting content for the world to see, would entail its risks and the individuals themselves are responsible for opening doors to multiple ways of content misrepresentation. But does this "public" privacy setting justify the untrackable sharing and reposting of content that the user has deleted or archived? Is it ethical to have someone's data stored in the ecosystem even after they have deleted it, just because it was posted "publicly"? Thus, the right to privacy on the internet and its intersections with the right to be forgotten has been a discussion inviting multiple views.

SNS comprise a huge amount of personal information marking the users' identity. It is conventional to have concerns regarding privacy on such platforms. While a few SNS like Reddit and YouTube allow non-members to engage on their sites and view users' information without registration, most widely used platforms like Facebook, Twitter, and TikTok require their users to provide a defined set of personal information for account creation and future interactions. Although these platforms offer numerous advantages to users, built-in online tracking methods are seen as a serious concern that affects SNS users. Online tracking on SNS could be seen as a way that helps platforms create a personalized experience for each user but the lack of transparency in the data collection process has led to the rise of privacy concerns amongst SNS users (Ur et al., 2012). Despite these concerns, interestingly the number of social media users is increasing every year (Kemp, 2022). While anonymity is also a choice for users to maintain their privacy, it was found that most people like to be known and seen online (Jones et al., 2020). Besides keeping an anonymous account online, there are various privacy settings in different SNS that have made it possible for users to disclose their data to selective audiences, giving a choice

to keep the personal information private (Poddar et al., 2009). For example, Instagram stories have a setting called 'Close friends' where you can choose to publish media content only among a group of mutuals the user picks. In addition, if the user doesn't want to share their content with a few people, Instagram also has a 'Hide story from' setting. In the case of Facebook, users have control over who can send them Friend requests, who can see information on their profile and they can even customize the visibility of individual posts. According to research on information sharing and privacy on Facebook, it was seen that users join SNS and disclose big amounts of personal information even though they are concerned about data privacy (Acquisti et al. 2006). However, disclosure choices like 'Friends only' options are found to be related to growth in levels of interpersonal privacy control (Stutzman et al., 2010). Previous research even found that users willingly share personal information despite being aware of the privacy dangers involved, primarily if the expected benefit is larger than the expected risk (Lee, Park & Kim, 2013).

Awareness of personal data privacy in regard to existing privacy policies on SNS

Amidst the booming number of connections and activities that we take part in online, there is undoubtedly a lot of unimaginable data flowing across platforms. Liking a page on Facebook, saving a product offer for later on Instagram, engaging in group discussions, interacting with public threads on Twitter, or even reading a whole article online, knowingly or unknowingly, we all leave a digital trail behind. A user is referred to as a data point in the framework of the data economy in SNS. A digital footprint means the collective information about a user online as a result of their online activity. This information is collected by websites, with or sometimes even without the consent of users.

The majority of the SNS that we use are free - or are they? Technically, they do not charge us a monetary amount directly to get access to most of their features. But users become a part of their advertisement-based business model. User digital footprints are circulated among advertising agencies that analyze the patterns and present targeted ads to the users - ads that generate the revenue for ad-based SNS. Accessing digital footprints always raises a question of the right to privacy (Cinar, N., & Ateş, S.,2022). This framework has given rise to the controversy of mining user data to target ads on SNS to manipulate users in decision-making - all this in exchange for "free" services on SNS. There have been multiple questions that surround this advertisement-based business model. Are SNS actually free? Are we being monetized to get access to it? How much of our data do we have control over? Is it acceptable for them to sell our data to third-party companies for profit? Should we be deleting our social media accounts? Or are we wrong in opposing a simple form of targeted marketing on these sites? Does the convenience of connecting with friends and accessing worldwide resources justify the unlimited use of our personal data? Back in 2011, an Austrian Law Student filed 22 complaints against Facebook using the Irish data privacy law, starting a whole campaign "Europe vs Facebook" which

ran for 6 years. He maintained a record of Facebook's illegal practices where it collected and marketed users' personal data, often without consent. He even highlighted how his deleted data was being retained by Facebook (O'Brien, 2012). The Irish Data Protection Commission (DPC) then undertook an examination of Facebook Ireland Ltd.'s data policy in accordance with the law at the end of 2011. Although the campaign had to take back all 22 complaints at the end of 3 years due to issues with the Irish DPC, the campaign has been a crucial step in exposing the loopholes in the Privacy Policy of Facebook. Fast forward to 2018, the Cambridge Analytica Scandal helped connect the dots on the effects of the leakage of Facebook user data in events like political campaigns. These discussions were later fueled by documentaries like The Social Dilemma on the popular streaming site Netflix in 2020. The documentary made it much simpler for the general public to understand the web of social media strategies and manipulations that they are entangled in (Barnet & Bossio, 2020). However, it is worth noting that the platforms mentioned in the documentary didn't abruptly collapse as an aftermath. The viewers have become alert but most users are still actively using them despite knowing the consequences. There seems to be a "dilemma" in the real sense - whether or not to use social media platforms even after knowing what goes behind them.

SNS surely have their privacy policies as well as terms and conditions (herein referred to as ToC) documented and presented to their users at signup, which detail the various uses of user data and its whereabouts. But an analysis of 150 privacy policies of popular social apps concluded that these documents are verbose and full of legal jargon, making them incomprehensible for a normal user to understand (Litman-Navarro, 2019). Another study in Europe showed that only one-third of their respondents claimed to understand privacy statements fully (Hallinan, Friedewald & McCarthy, 2012). Others stated, there was a considerable lack of comprehension as to what they represented or what they meant when read in full. With ambiguous and unclear privacy guidelines slapped at signup pages of SNS as mandatory agreements, users are bound to agree to conditions to get access to these platforms at the expense of losing their control over digital privacy. As an aftermath, users resort to maximum utilization of privacy customization options to control the spread of their data. But interestingly a study in New Zealand showed how despite repeated warnings of data disclosure risks, social media users make their own decisions about information disclosure without fully considering the user agreements, putting themselves at risk because they want to be a part of these communities and open up about themselves to strangers (Aljohani, Nisbet & Blincoe, 2016). Thus, the discussions around digital data privacy - specifically deconstructing legal language in policy documents on SNS and laying out crucial information on user data whereabouts with clarity, are of utmost importance.

Privacy on SNS in the context of Nepal

If we shift from the global perspective back to the context of Nepal, data privacy would seem to be a myth. Nepal lacks any platform-specific regulatory laws and it has been pointed out

repeatedly that the Data Privacy Act 2075 misses out on a lot, specifically in issues like the lack of right to access data of data subjects, lack of right to erasure, and the right to opt-out (Chopra & Bareja, 2022). Due to this, the concept of regulating the monetization of data on social media platforms might seem like a far-catch. Nevertheless, with ever-so-changing technology and the majority of Nepali users moving their presence to SNS, it is crucial to understand where SNS users stand on the spectrum of having control of their data.

Emerging adults between the age of 18-29 are one such age group who have grown with technology and have been first-hand witnesses to the benefits and risks of modern SNS today. People from this age group are the most active consumers of social media as well as producers of big data on these platforms (Pew Research Center, 2022). Research also states that younger age groups (18-24 years) are more conscious of privacy issues online (Kaiser A.F., 2016). While there exists data on active SNS users and their most used SNS, their preferences on information disclosure and its relationship with their privacy settings have rarely been studied in the context of Nepal.

Objectives

The purpose of this research was to understand how the youths of the age group 18-29 perceived privacy concerns associated with SNS. In addition, we wanted to understand the relationship between users' personal privacy preferences on SNS and their willingness in providing data to third-party services. Through this study, we aim to meet in particular the following objectives:

1. User online engagement patterns on SNS
2. Attributes affecting a user's privacy preferences on SNS
3. Relationship between the amount of information people disclose on social networking sites and their level of privacy concern regarding data collection on these platforms
4. User understanding of how their personal data is secured by social media platforms in accordance with the privacy documents they have accepted

Methodology

To fulfill the aforementioned objectives, we carried out a survey among 377 participants within the age group of 18-29, using a questionnaire consisting of 41 questions. The population was selected on the basis of two sampling techniques, viz. Convenience sampling and Snowball Sampling. Further, surveys amongst the students from three schools, Birendra Multiple Campus, Wave Institute, Shree Durga Sheshkanta Adhikari Secondary School, and Shree Dhadaghari Secondary School in the Chitwan district were administered in person through paper distribution. The surveys were also conducted through an online form where we had requested the

respondents to pass on this survey to their acquaintances and anyone falling under the demography we wanted to understand.

The questionnaire for the survey was sectioned into the following sections:

a. **Social media usage and engagement patterns of the user**
   This section was put in order to identify the engagement patterns of the users in social media. It included some open-ended questions like how much time did they spend engaging on social media and the number of social media apps they frequently used. It also included some close-ended questions to understand the frequency of social media usage of the participants and the type of content they posted on these platforms. This information was helpful to analyze if engagement patterns and social media usage affect user privacy concerns on SNS.

b. **Privacy maintenance techniques of users on social media platforms**
   This section included some close-ended questions to understand the approaches of the survey participants to maintain some level of privacy on the social media platforms they use. It also had some questions to understand the type of information people are willing to provide on social media platforms.

c. **Data collection on social media platforms.**
   This section included mostly close-ended 5-point Likert scale questions which were helpful in understanding the concerns of the survey respondents and their level of awareness regarding data collection by third parties on SNS.

Limitations

The small sample size deters the findings to be generalized to the broader context. However, with a modest sample size, the queries the respondents had regarding the survey, were addressed well. This has contributed to the accuracy of their responses. There was also a lack of previous studies and research on data privacy that was conducted in Nepal. The gap in the literature was bridged with the help of international resources.

In our research, the phrase 'Terms and Conditions' is used as an umbrella term for any piece of writing offered by SNS to ask for users' consent, which also details the flow of user data in the platforms. Due to this, it is not in the scope of the research to find out if the respondents have clear knowledge about privacy policies, ToC, and application permissions separately. The scope of the research is also limited to respondents' personal choice of SNS. The privacy synopsis of SNS that was not used by the respondents is completely excluded from the results. Regarding the usage time of SNS, the ambiguity of the term "usage" might have resulted in varying results.

Some respondents consider the act of playing music on Youtube in the background as usage, hence adding up to their social media hours. Hence, the reflection of social media hours might not be the most accurate of the average amount of time spent on SNS.

Demographic Composition of the Sample Population

The survey responses were cleaned and a few basic pieces of information from the data was extracted which were also helpful to generate findings to meet the objective of this research. Some of these are mentioned below:

1. Distribution of age group of survey respondents

Around 37.14% of the participants belonged to the age group 18-20 while another 30.77% belonged to the age group 21-23. 25.2% of the participants were between 24-26 and the remaining 6.9% were between 27-29.

2. Distribution of district

Where do you live?	Number of participants
Province 1	13 (3.45%)
Madhesh	22 (5.84%)
Bagmati	257 (68.17%)
Gandaki	55 (14.59%)
Lumbini	24 (6.37%)
Karnali	1 (0.26%)
Sudurpaschim	5 (1.33%)

Table 1: Distribution of geographic origin of our survey respondents by province

3. Distribution of any disability

Around 4.5% reported to have some form of mental disability while 3.7% reported to have some form of physical disability.

4. Distribution of gender identity

Distribution of respondents on the basis of gender identity showed that about 58.9% of them were Cis women, 37.7% were Cis Men, 1.9% belonged to the Non-binary or Gender-Diverse group and less than 1% were Trans people.

5. Distribution of sexual orientation

Survey participants were divided into groups based on their sexual orientation and we observed that around 52.5% were heterosexual women and 40.05% were heterosexual men. Also, 2.39% of them were asexual, 1.59% of them identified as pansexual or queer, and less than 1% identified themselves as bisexual.

6. Distribution of professional fields

About 60.14% of respondents who were working professionals were from IT and engineering backgrounds, 8.7% of them were from Business, Administration, and Management backgrounds, and 7.24% of them were from healthcare and medicine backgrounds. The remaining 23.9% of the respondents were from backgrounds other than mentioned above.

7. Distribution of students and professionals

Around 11.94% of the involved participants were both working professionals and students. 62.33% of the total respondents were students while 24.4% of them were working professionals.

Findings

1. User online engagement patterns on SNS

When we tried to understand user engagement patterns and activity on SNS, the following findings were revealed:

a) Time spent on social media in hours

Among our respondents, it is seen that the highest number (47.74%) spend 4 to 7 hours on social media, followed by 40.58% of respondents who spend 3 hours or less on a daily basis. It is seen that SNS has become an inevitable part of everyday life. The number of hours spent on SNS was found to be mostly for connecting with friends and family, consuming digital content, and posting personal life events and updates according to a question asked in our survey.

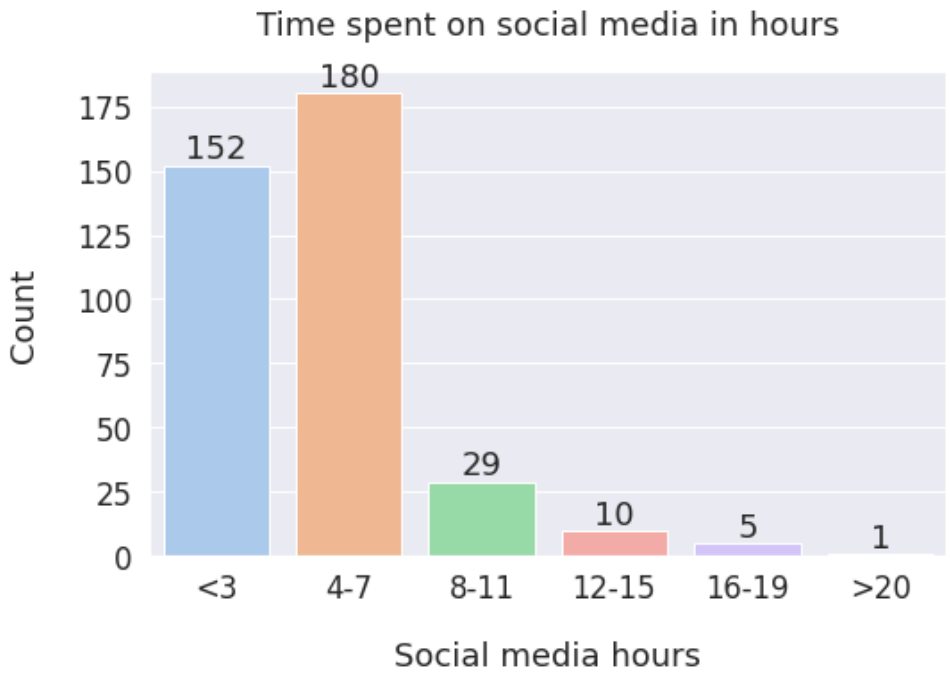

Figure 1: Time spent by our respondents on social media in hours

b) Frequency of posting on SNS

The survey tried to observe how often people post on SNS. It is found that most people prefer to share the content as often as 1 to 4 times a week (27.85%), once every month (22.01%), to at least once every few months (27.05%). Only 9.28% of people choose to post once a year or less. This shows that more people are inclined towards posting their content on SNS very commonly.

c) Distribution of top 3 apps

While surveying our participants, we asked them their top 3 most commonly used SNS and most of them mentioned Instagram, Facebook, and YouTube to be their top favorites. Out of 377 respondents, 263 of them used Instagram, 254 used Facebook, and 210 used YouTube.

We observed that even Tiktok was quite popular and around 176 of the respondents used Tiktok while a small population also used social media apps like Twitter, LinkedIn, Pinterest, Reddit, and Clubhouse.

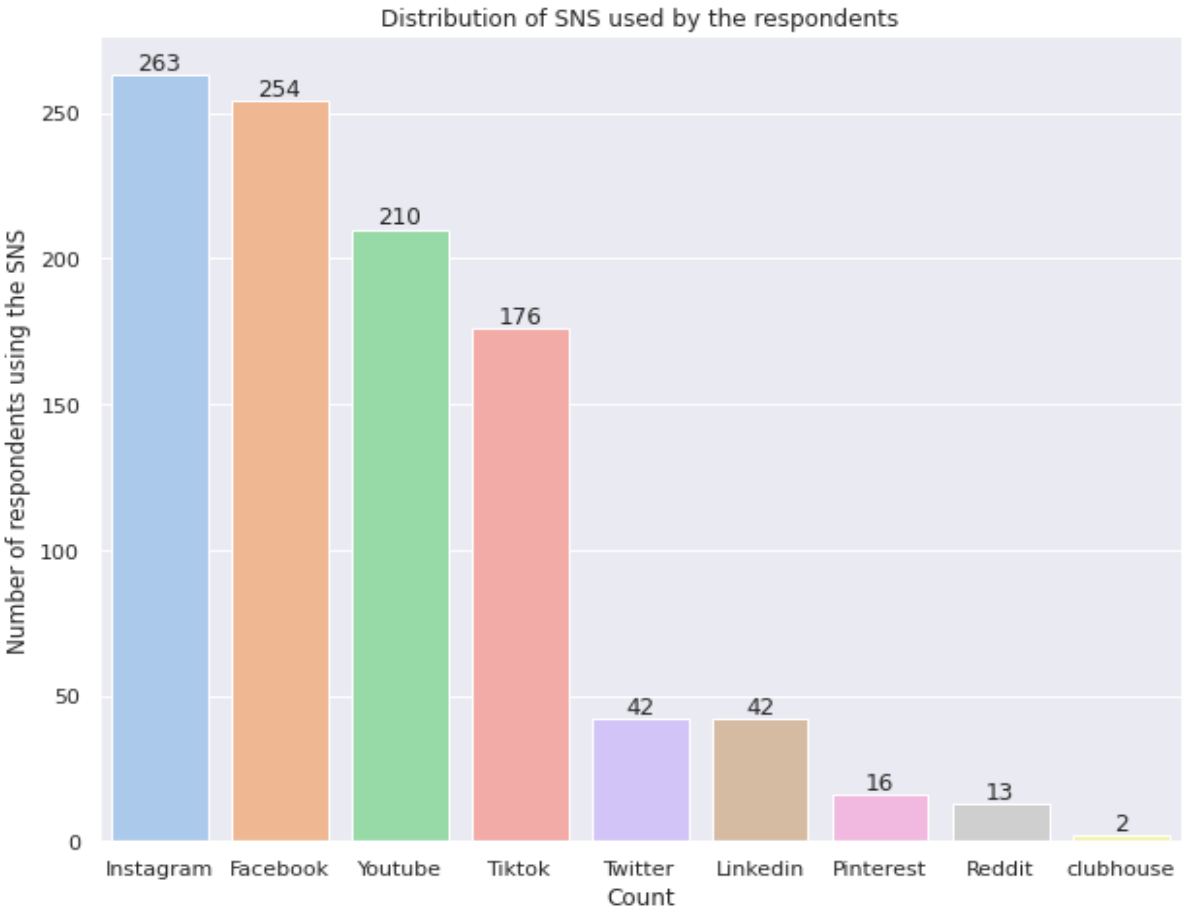

Figure 2: Distribution of SNS used by the respondents

d) Distribution of top 3 messaging platforms

The most commonly used messaging app by our participants was found to be Messenger, Instagram, and Whatsapp. Around 332 participants mentioned Messenger. 215 mentioned Instagram and 142 mentioned Whatsapp to be their most commonly used messaging app.

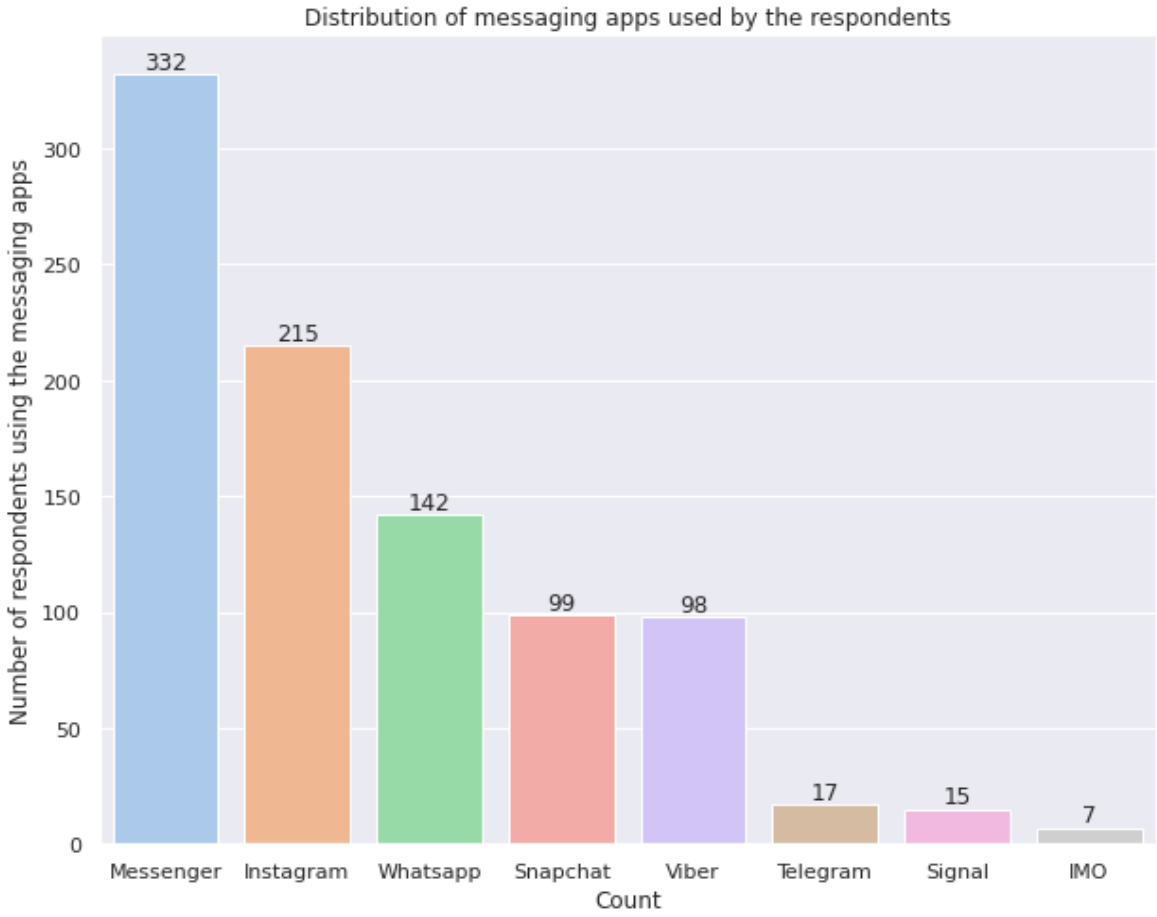

Figure 3: Distribution of messaging apps used by the respondents

e) Frequency of updating personal information on SNS

A social media account can consist of many personal information like birthdate, address, relationship status, work, hobbies, and others. It is seen that the respondents do not prefer to update their personal information very often on SNS. 36.60% of people update it only when it is needed, followed by 27.58% of people who update their personal information at random times only when they feel like it. It is also found that 18.30% of the respondents never update any personal information on social media which is higher than people who immediately update (7.69%) and those who timely update (9.81%).

f) Frequency of filtering contacts on SNS

When asked how often they filter their contacts on SNS, we discovered that the majority of them did not prefer to filter them very frequently. While 38.99% of the respondents do it once a year or less and 30.23% choose to do it once every few months, only 2.19% filter their contacts every day. This might be a result of

people being careful when adding contacts to their social media platforms so they don't have to constantly screen them.

How often do you filter your contacts on SNS?	Number of participants
Very Often (Daily)	2.92%
Often (1-4 times a week)	11.67%
Moderately (Once every month)	16.18%
Rarely (Once every few months)	30.24%
Very Rarely (Once a year or less)	38.99%

Table 2: Frequency of filtering contacts on SNS

g) Frequency of deleting data on SNS

When respondents were asked about how often they delete or hide their past contents, it was seen that 226 out of 377, that is more than 50% of the respondents, delete their posts frequently. The respondents mentioned that they find their past contents irrelevant or embarrassing.

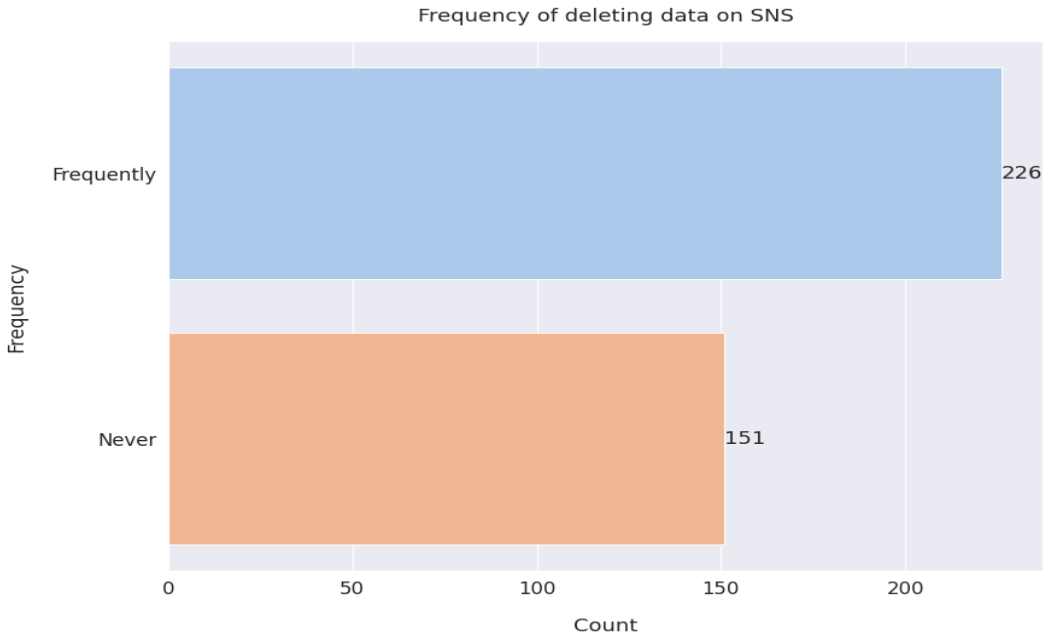

Figure 4: Frequency of filtering data on SNS

2. Attributes affecting a user's privacy preferences on SNS

The data on the matters of preferences of private accounts over public accounts revealed that:

a) Users prefer private accounts over public ones, irrespective of their age, gender, sexual orientation, the field of study, or current positions.

   For some, it also depends on the type and nature of SNS, but there are a very small number of users with public accounts. While sociality through social networks might seem like a public process, people still prefer to keep it within their closed groups.

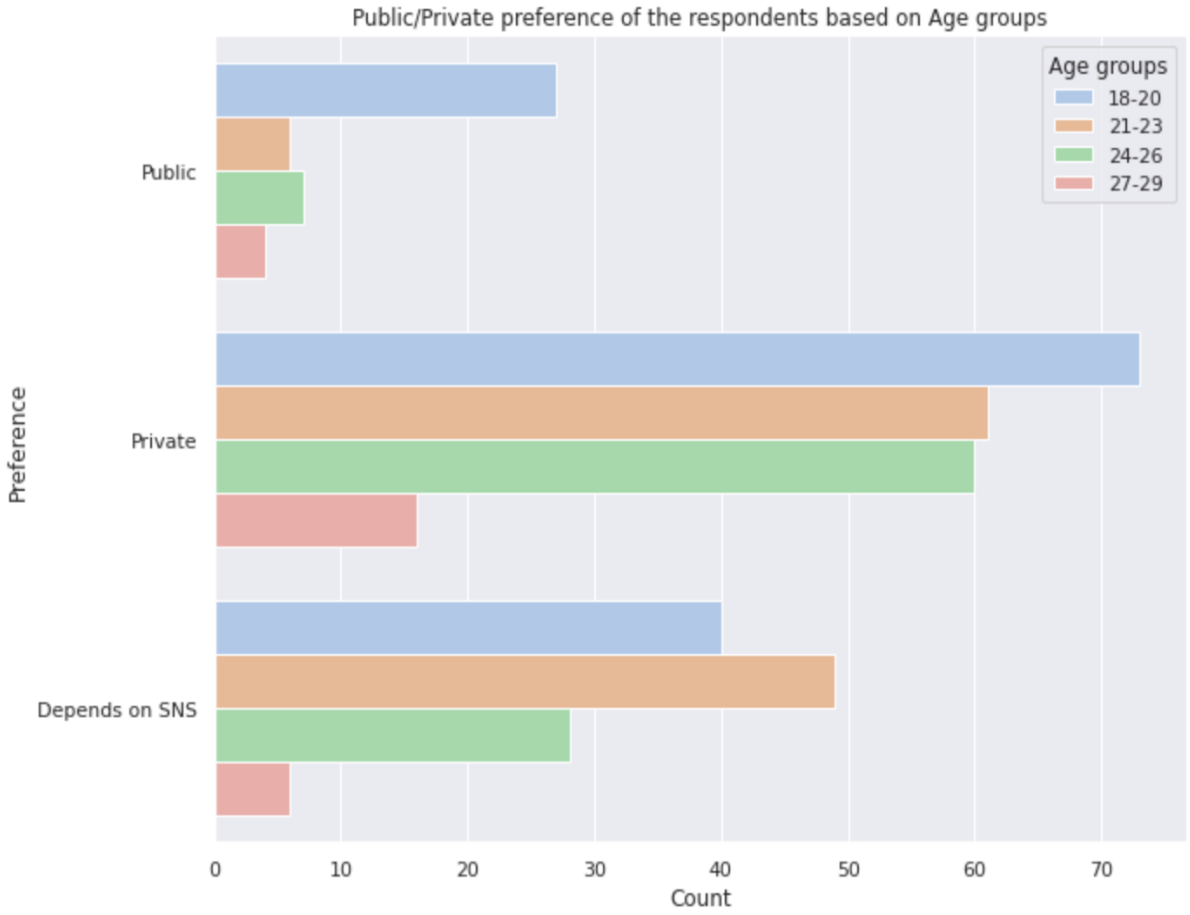

Figure 5: Public/Private Preferences of the respondents based on age groups

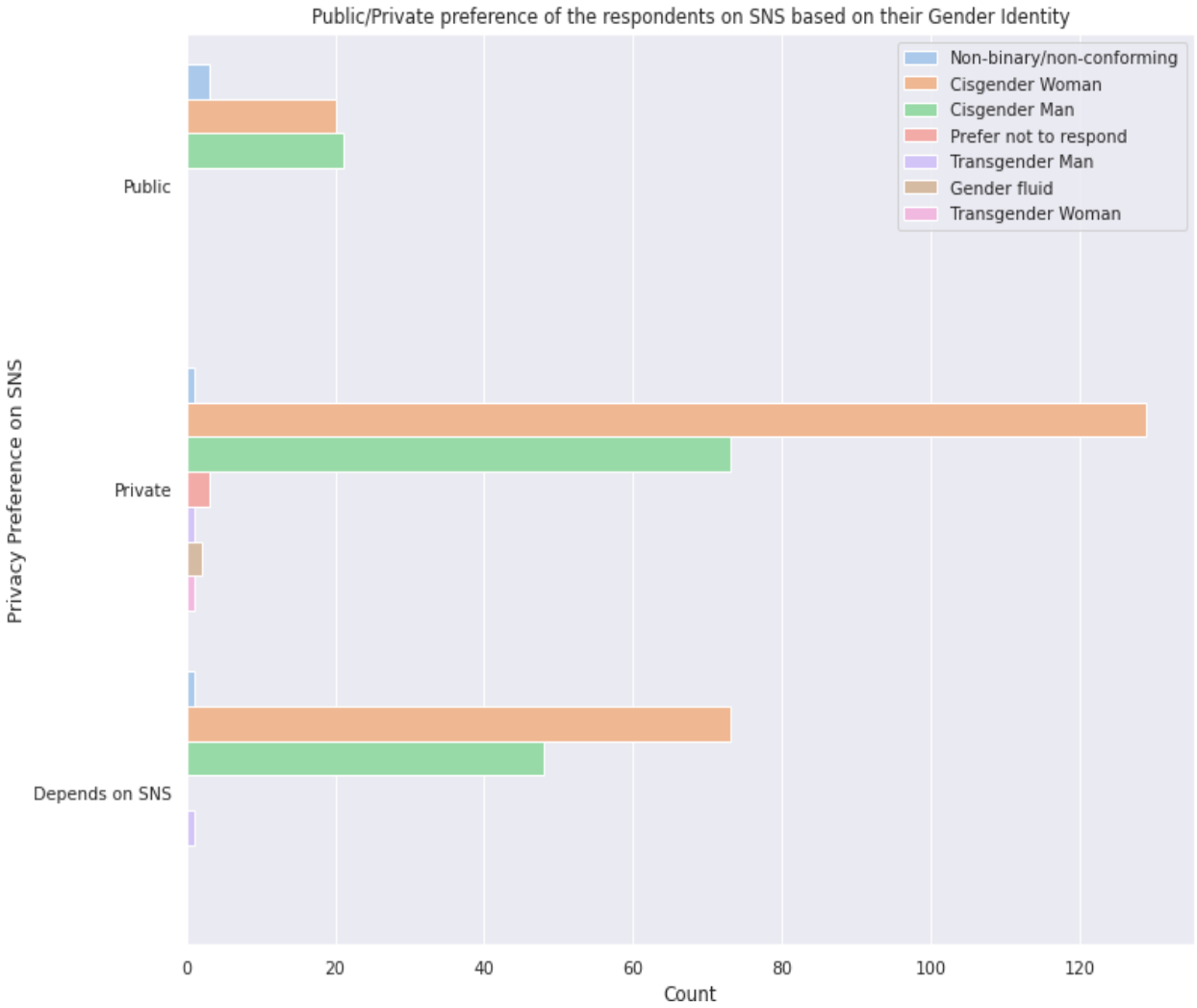

Figure 6: Public/Private preference of the respondents on SNS based on their gender identity

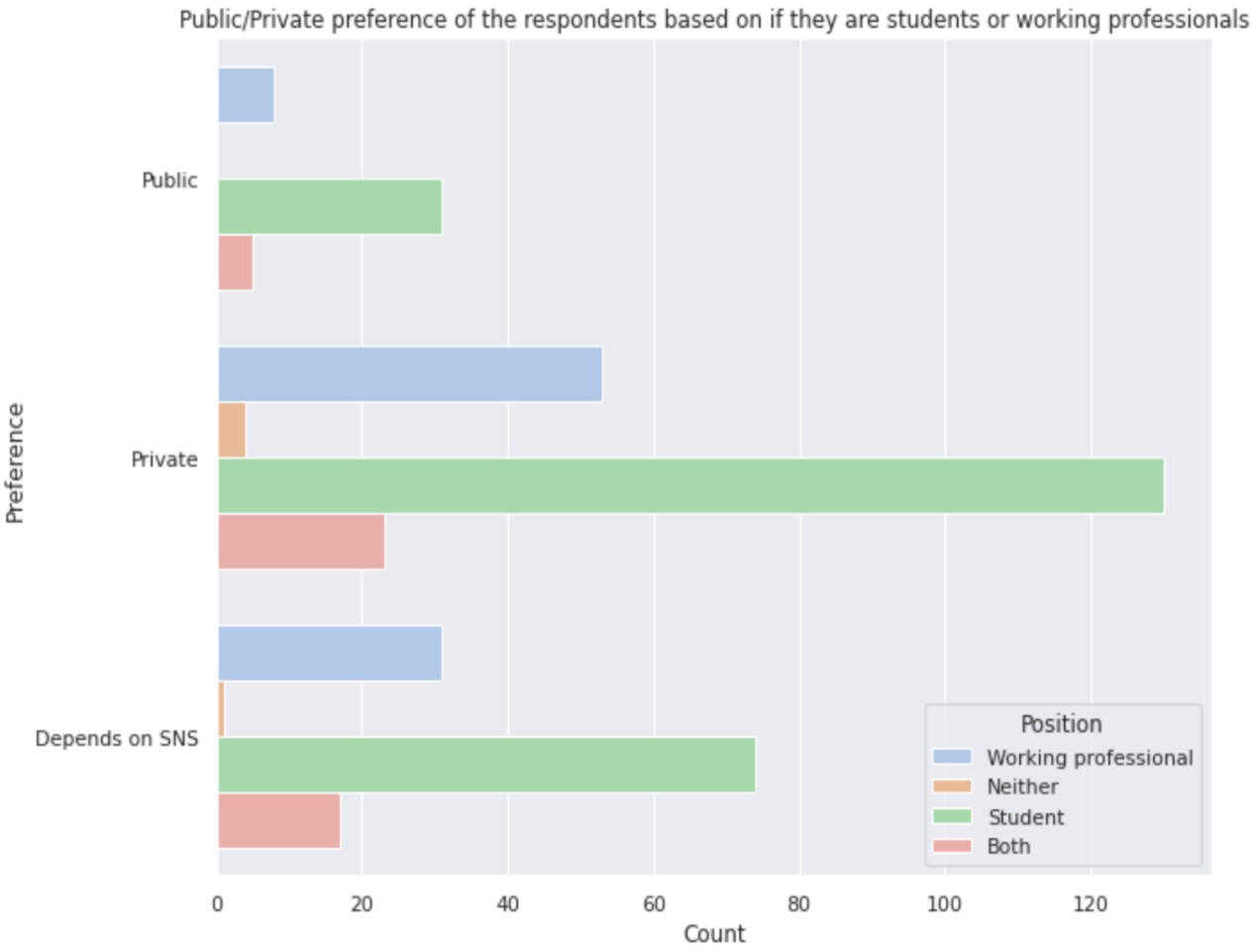

Figure 7: Public/Private preference of the respondents on SNS based on whether they are students or working professionals

b) The age of SNS users is one of the factors determining public/private preferences.

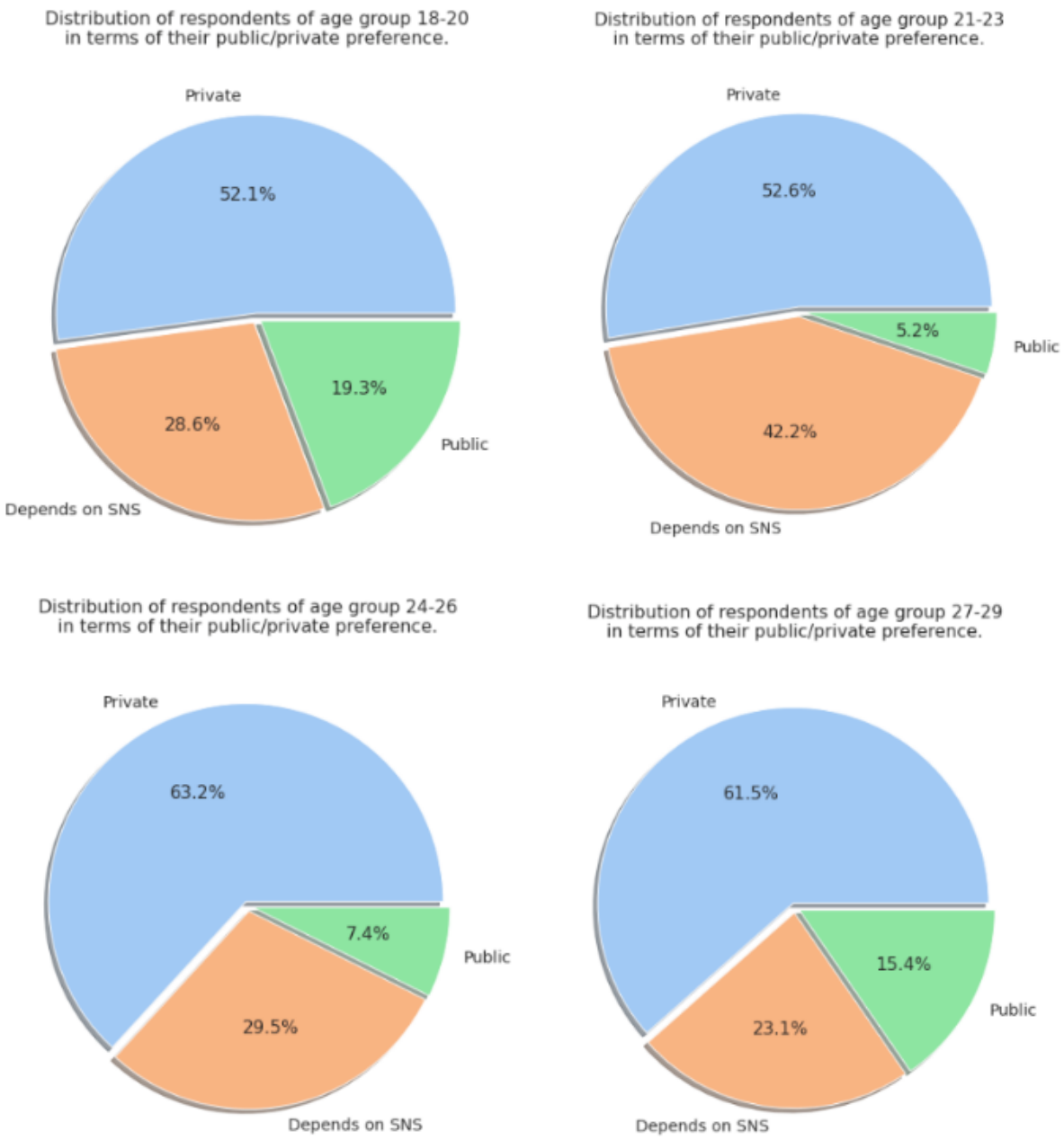

Figure 8: Distribution of respondents of varied age groups in terms of their public/private preferences

Though most people in all groups prefer private accounts over public ones, the percentage of private accounts is higher by about 10% for people after 24 than the ones who are in the age group 18-23. This resonates with the research conducted on about 3.2 million mobile phone users on Sex Differences in Social Focus across the Life Cycle in Humans, which concluded that people were socially engaged, active, and outgoing up until the age of 25, continuously forming new friendships and social ties (Bhattacharya et al., 2016). Since they are open to new connections in real life, they can be more open to connecting with people, either known or unknown, on SNS. Consequently, we can say that one of the elements influencing privacy settings is the age of the SNS user.

c) Distribution of respondents belonging to different gender in terms of their public/private preferences.

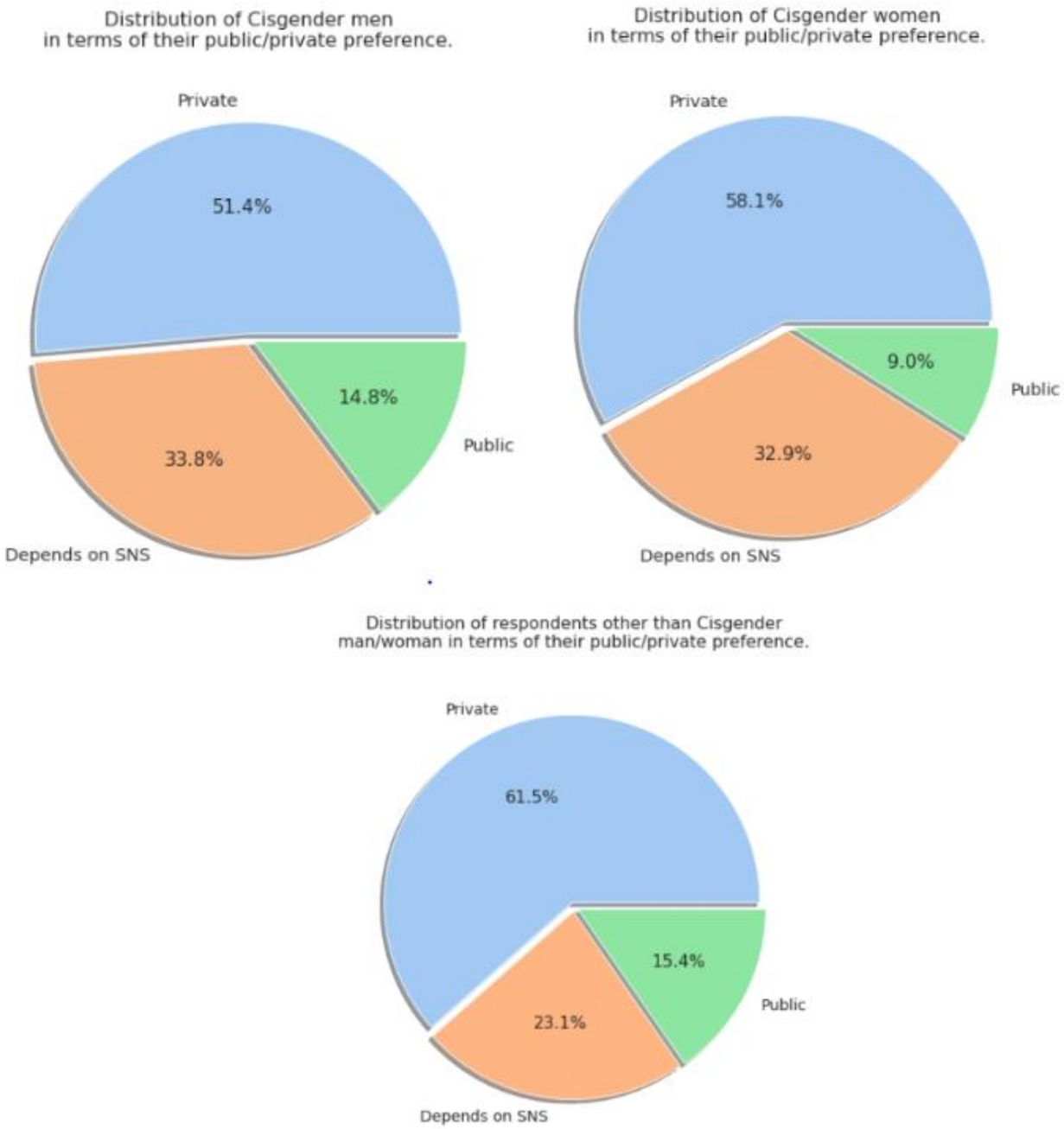

Figure 9: Distribution of respondents belonging to different gender in terms of their public/private preferences.

The comparison of privacy between respondents of different gender identities revealed that cisgender men tend to remain least private with 51.4% in private preference, 58.1% of cisgender women preferred private accounts and 61.5% of respondents with a different gender identity checked for a private preference.

d) The level of privacy concern directly affects public/private preference settings in SNSs.

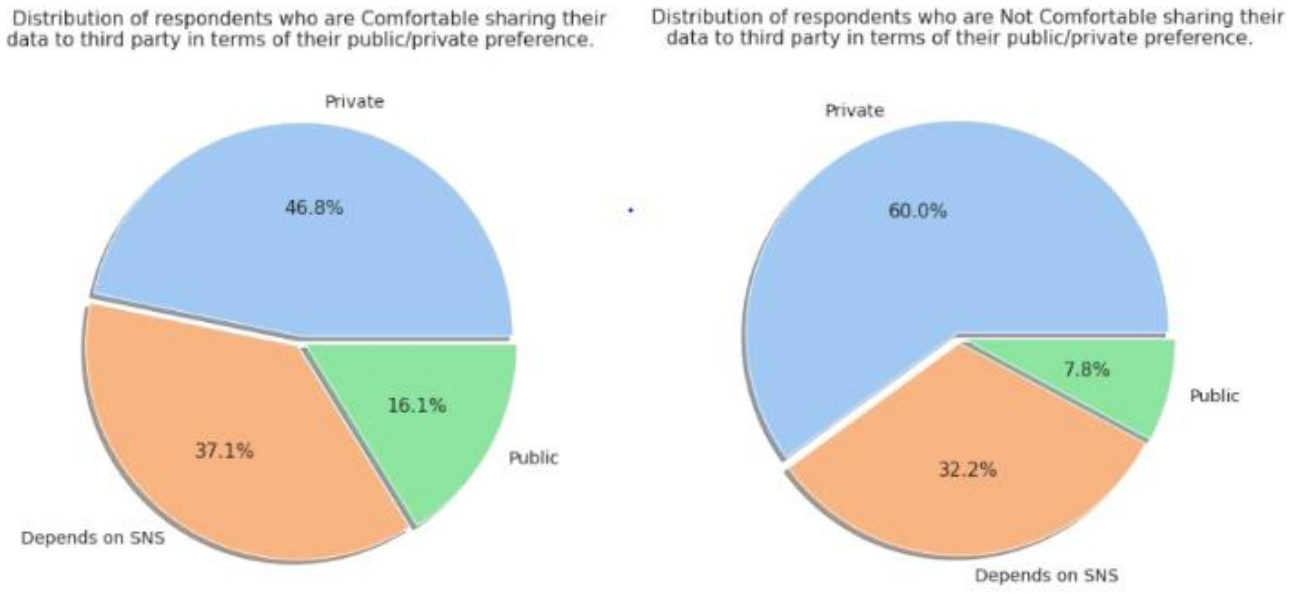

Figure 10: Distribution of respondents and their comfort level sharing their data to third-party advertisers in terms of their public/private preferences

From the first graph, it can be seen that 46.8% of people who were okay with sharing their data with third parties have private accounts and 16.1% of them have public accounts. While in graph 2, 60% of the people who are not comfortable sharing their data with a third-party application have private accounts and only 7.8% of them have public accounts.

Users that have strong privacy concerns are more likely to withhold their personal information from SNS or to provide it falsely (Sheehan, K. B., & Hoy, M. G., 2000). The level of privacy concern is directly related to the privacy settings of SNS users. People who are not comfortable sharing their data with a third party and are worried about data leakage, misuse of personal information, etc. tend to keep their accounts private.

e) People are hesitant to share real locations while posting pictures or videos.

How often do you add your real location on SNS?	Number of participants
Always	11.94%
Occasionally when needed	51.72%
Never, I don't like adding location information	36.34%

Table 3: Distribution of respondents and their location-sharing preference

The table demonstrates that many people dislike disclosing their actual locations. Most of the respondents either don't like sharing their information at all or are okay with sharing their locations occasionally when needed.

There may be safety concerns with posting your location on social media (Cohen, S., 2016). What if you added a check-in every time you visited a new place? Your whereabouts could be tracked using this information by burglars, robbers, and other evildoers, which could result in harmful, risky circumstances. Privacy settings and permissions, thus also depend on the type of permission you are granting to the application.

3. Relationship between the amount of information people disclose on social networking sites and their level of privacy concern regarding data collection on these platforms

a) Dynamics of Data Privacy with respect to anonymity

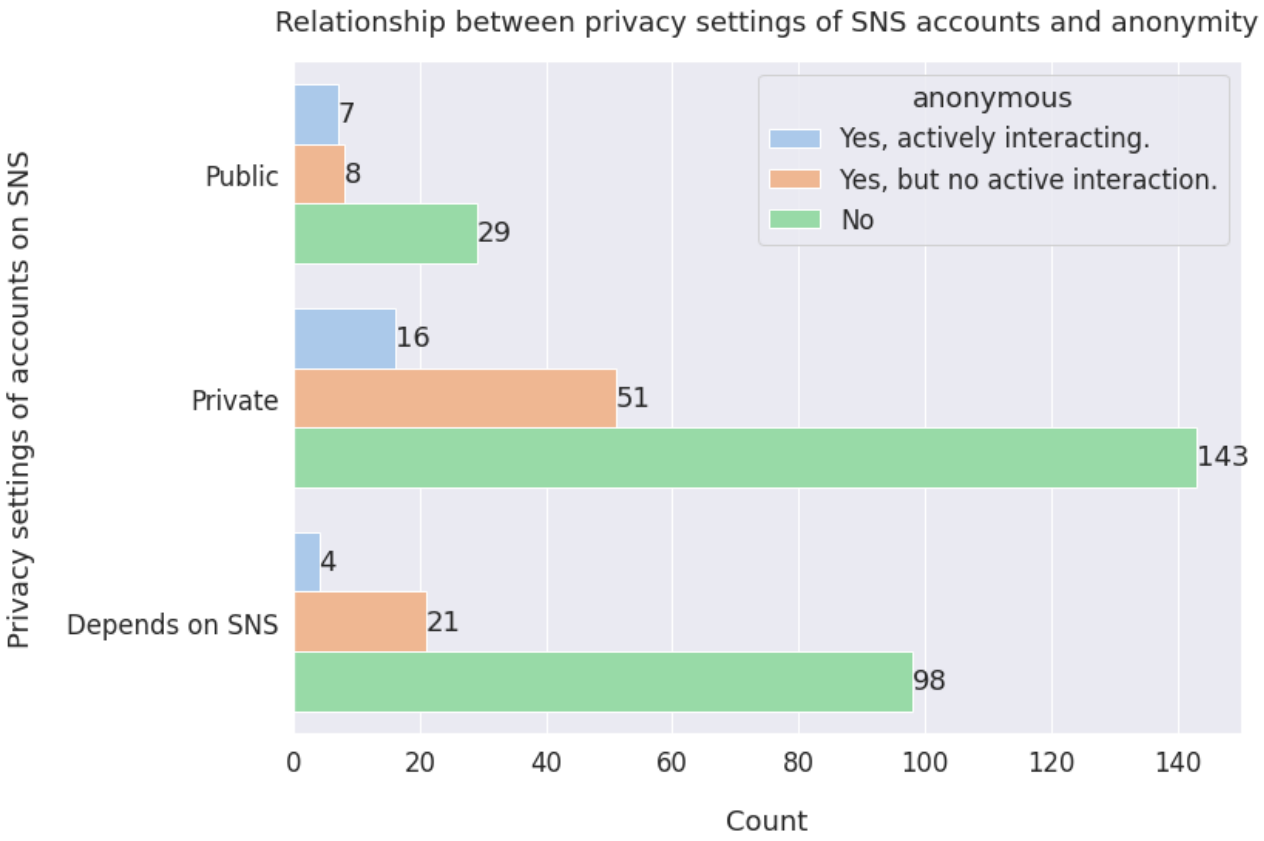

Figure 11: Relationship between privacy sessions of SNS accounts and anonymity

i. It can be seen that regardless of the privacy settings the users choose for their accounts, most of the respondents do not prefer to stay anonymous. Only 27 out of the total respondents said they actively use their anonymous accounts. This also aligns with the findings of research that shows a decline in the number of anonymous users created on SNS over years. (Jones et al., 2020).

When respondents were asked why they use social media, the majority of them said they use it to connect with their family and friends. Because most of their online interactions involve people they know in real life, this could be one of the reasons why SNS users do not prefer anonymity on these sites.

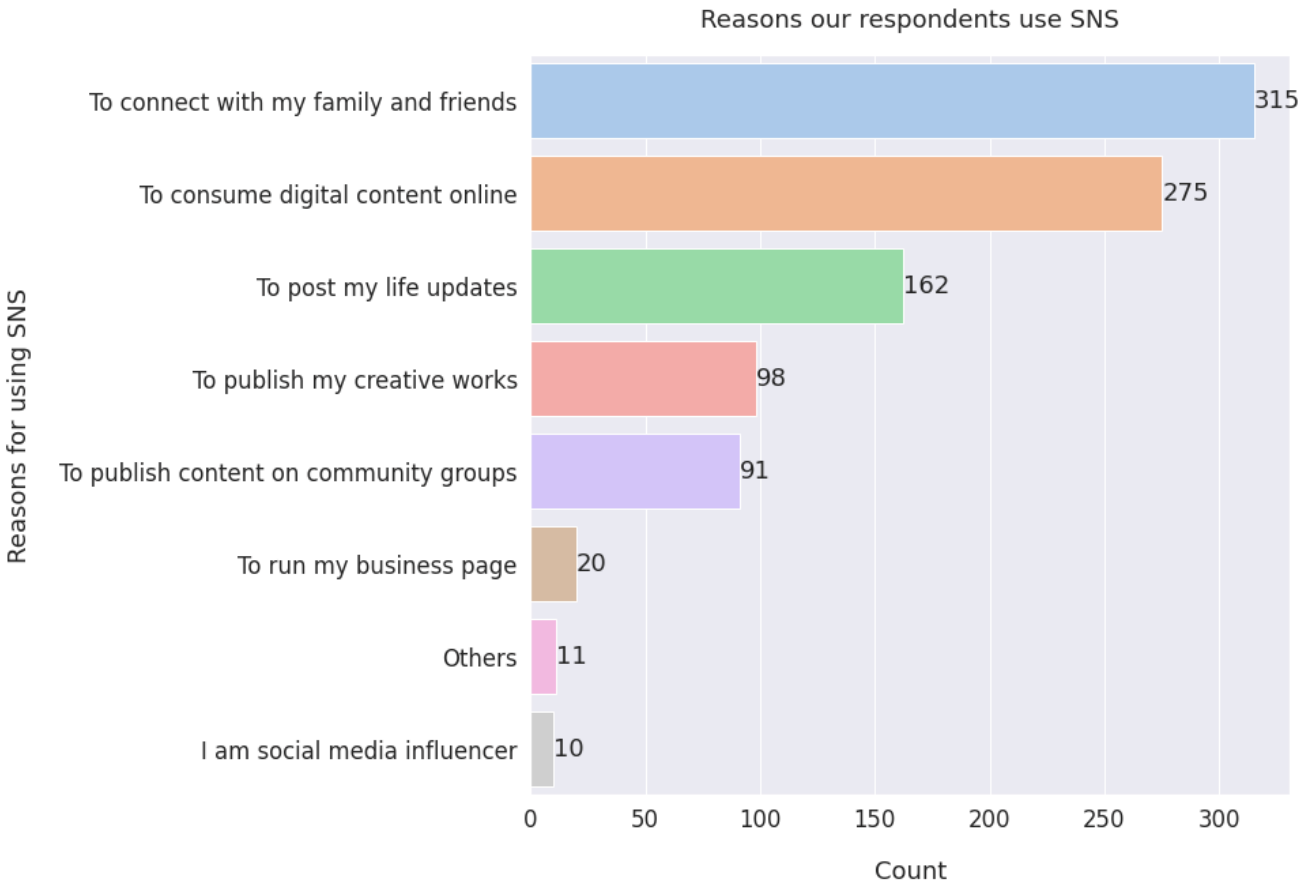

Figure 12: Reasons why our respondents use social media sites

ii. Choosing to stay anonymous in SNS prevents users from leaving digital footprints thus maintaining privacy. However, among our respondents who prefer staying anonymous, 53.6% do so for fun and no other reasons.

Why do you choose to remain anonymous?	Number of participants
No major reason and just for fun	53.60%
To keep my private information undisclosed	24.60%
To prevent others from tracking my social media activity	15.60%
Because society would hesitate to accept my real identity	6.10%

Table 4: Reason to choose anonymity on SNS

b) Privacy concerns in different social networking platforms

Among our respondents, most prefer to stay private on Instagram, a total of 249 respondents followed by Facebook where 215 respondents remain private. Furthermore, Youtube and Tiktok also have a significant number of private users, 104 and 96 respectively. This could be because these are platforms where users

heavily post visual contents that give personally identifiable information. The users might experience higher comfort limiting the content disclosure only to their friends.

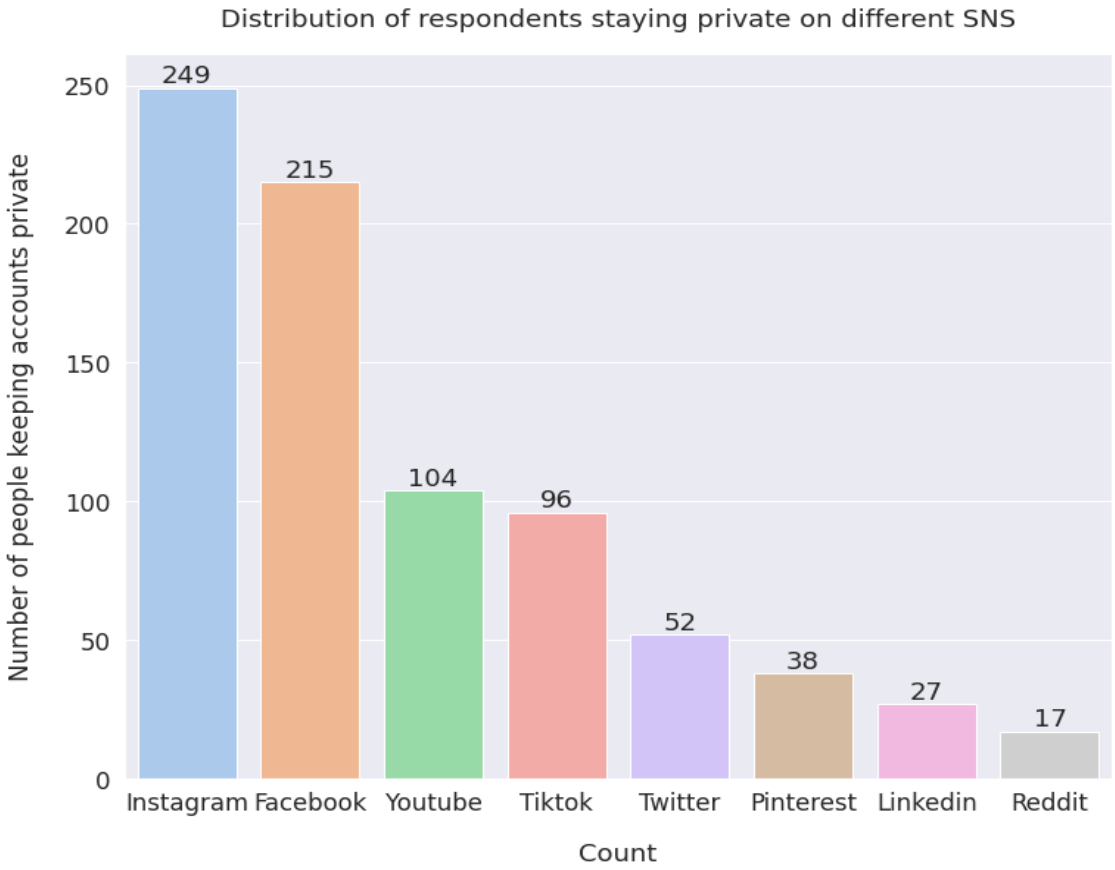

Figure 13: Distribution of respondents staying private on different SNS

c) Dependency of Level of privacy concern on the information SNS users share

i. According to a survey conducted on SNS users about their privacy settings and information disclosure, users are generally willing to use real names, disclose personal attributes such as dates of birth and hometown locations and often post personal pictures that could identify themselves, family members and friends in order to gain popularity, make friends and be a part of the community (Aljohani et al.,2016).

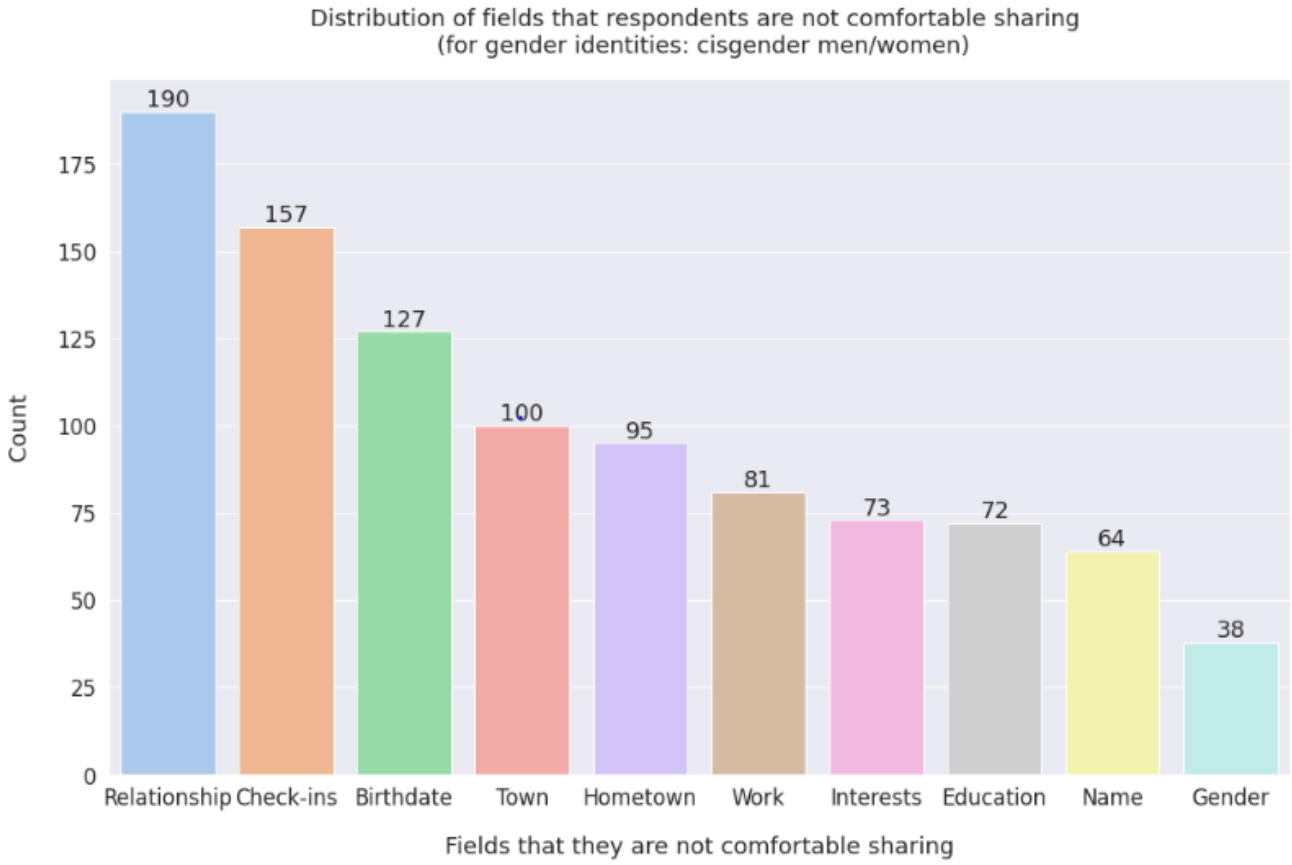

Figure 14: Fields that respondents who were cisgender men/women are not comfortable sharing

In the graph above, it is seen that most of our respondents **who identify as cis-gender men or women** are not comfortable sharing the fields like relationships, check-ins, and birthdates. The lowest number of total respondents stated they were uncomfortable disclosing their gender in SNS, while the highest number of respondents said they were uncomfortable sharing their relationship status.

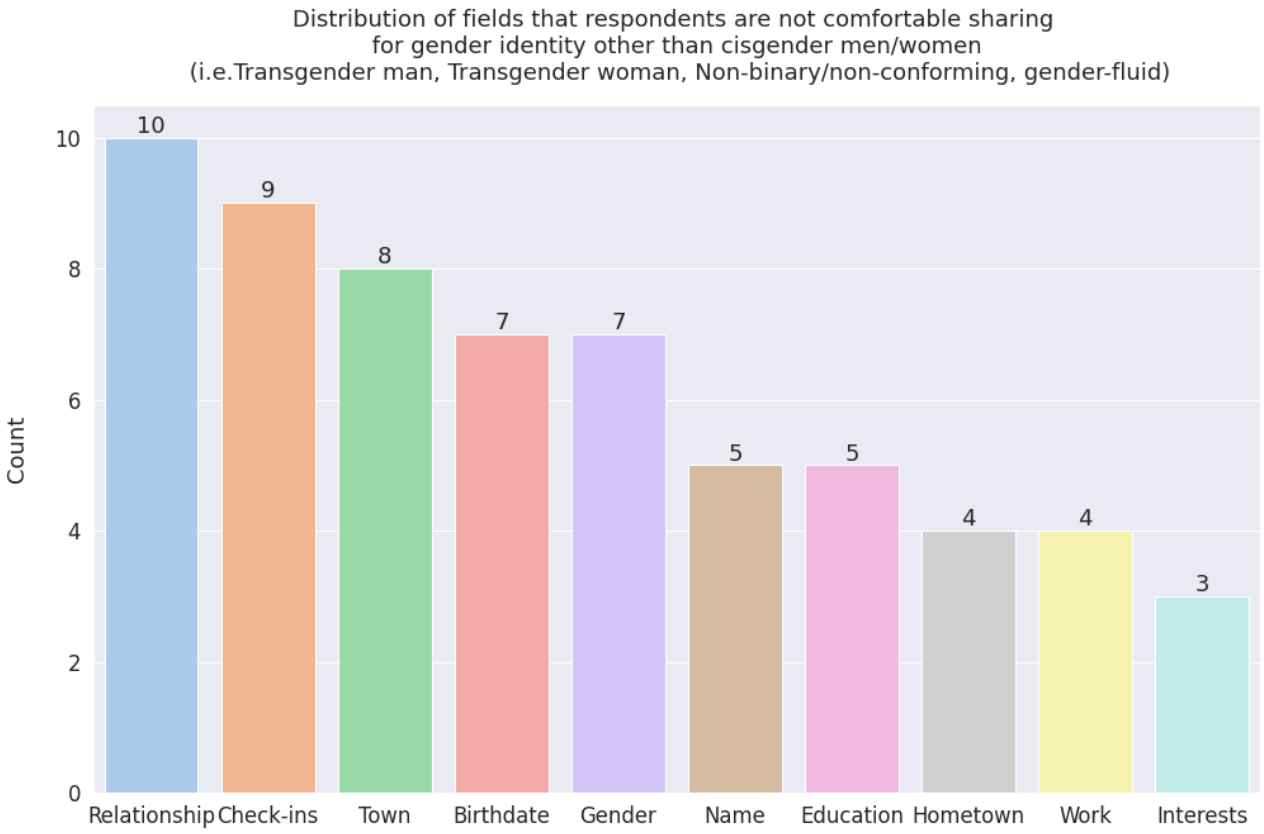

Figure 15: Fields that respondents of gender identity other than cisgender/cisgender women are not comfortable sharing

Analyzing the same questions for respondents with a **gender identity other than cisgender man/woman** (transgender man/women, non-binary, non-conforming, and gender fluid), we found a similar pattern on relationships and check-ins. However, it is seen, Gender identity falls under the fourth most-common field the respondents prefer hiding in SNS.

ii. If we look at the **type of posts shared by users having public accounts**, they included more personal visual information like photos and videos over text-based and public information.

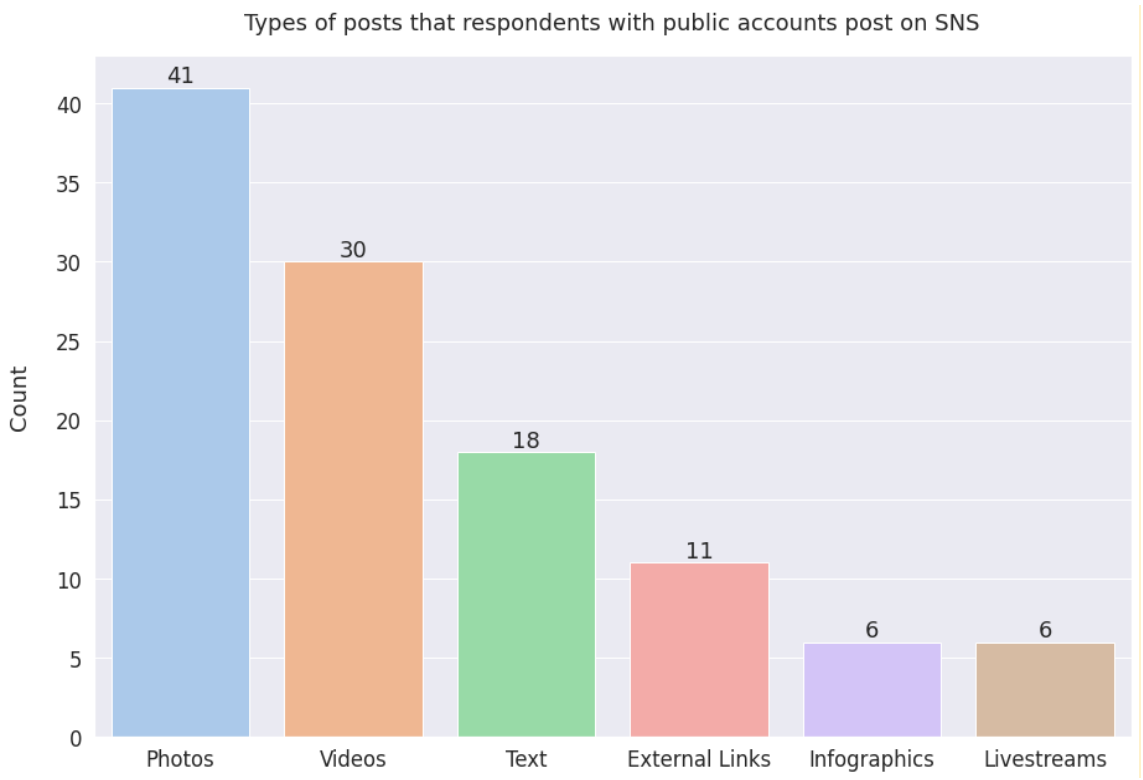

Figure 16: Types of posts that respondents with public accounts post on SNS

Interestingly, a similar trend is seen for the **type of posts shared by users with a private account**- they also prefer to share personal photos and videos contents over text-based and creative content. In a research by Stutzman and Kramer-Duffield in 2010, it was highlighted that privacy practices on SNS can appear paradoxical as content sharing behavior of the users conflicts with the aim to lessen disclosure-related damages (Stutzman et al. 2010). Personal photos and videos are directly connected to one's public identity and reputation, and sharing them in a private account creates a similar privacy paradox situation in SNS.

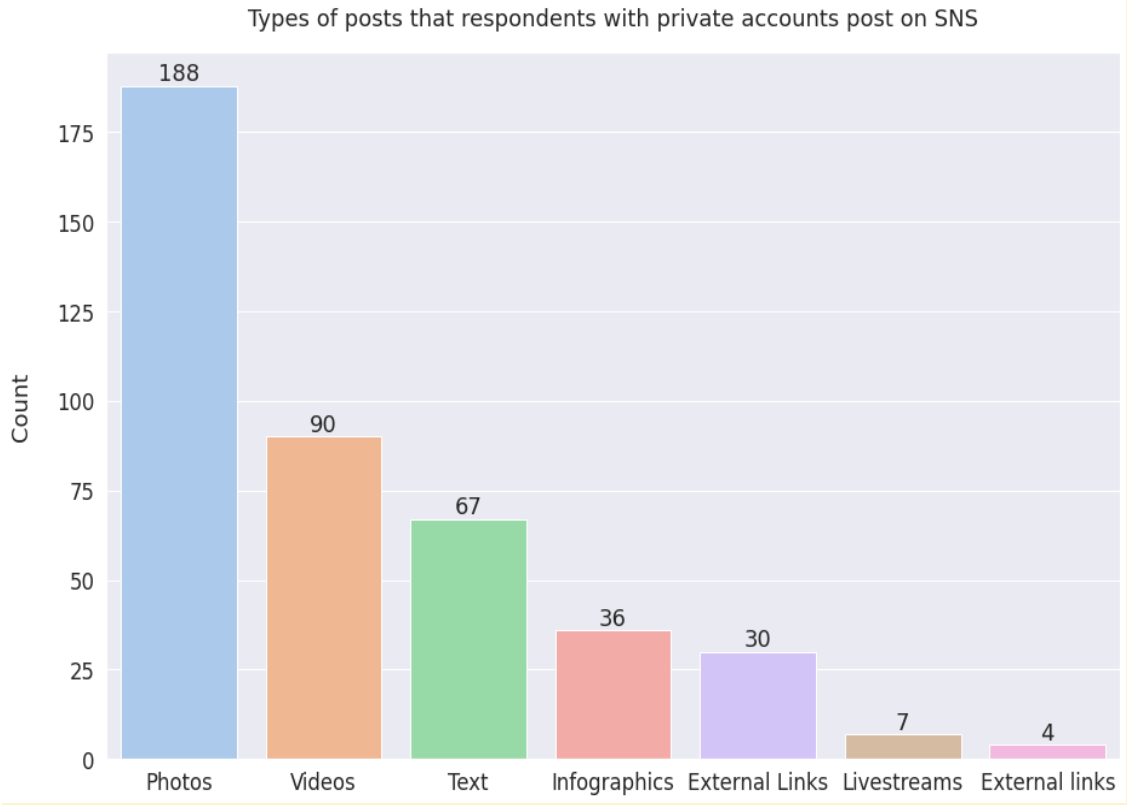

Figure 17: Types of posts that respondents with private accounts post on SNS

d) Understanding of encrypted messaging & messaging platform choices

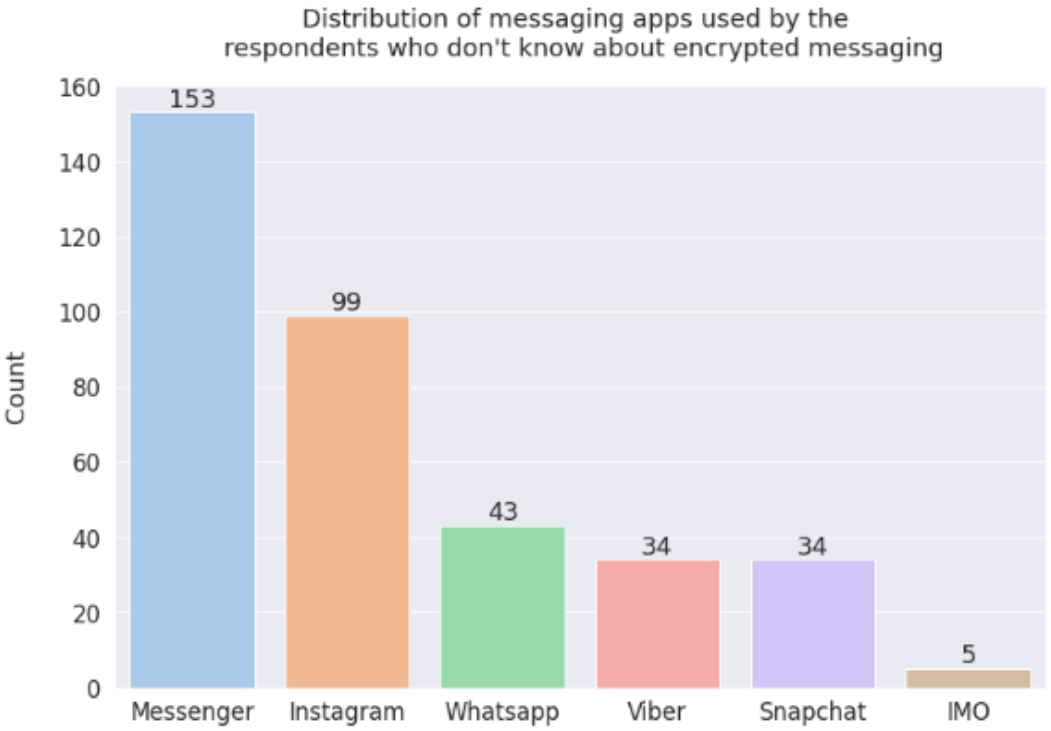

Figure 18: Distribution of messaging apps used by the respondents who know about encrypted messaging

We asked our respondents about their familiarity with encrypted messaging and messaging platforms they use. Those who didn't know about encrypted messaging used platforms like Messenger and Instagram which are non-encrypted by default over encrypted ones like WhatsApp, Telegram, and Signal. Messenger was the most commonly used platform followed by Instagram Messages. None of them used highly encrypted platforms like Telegram or Signal.

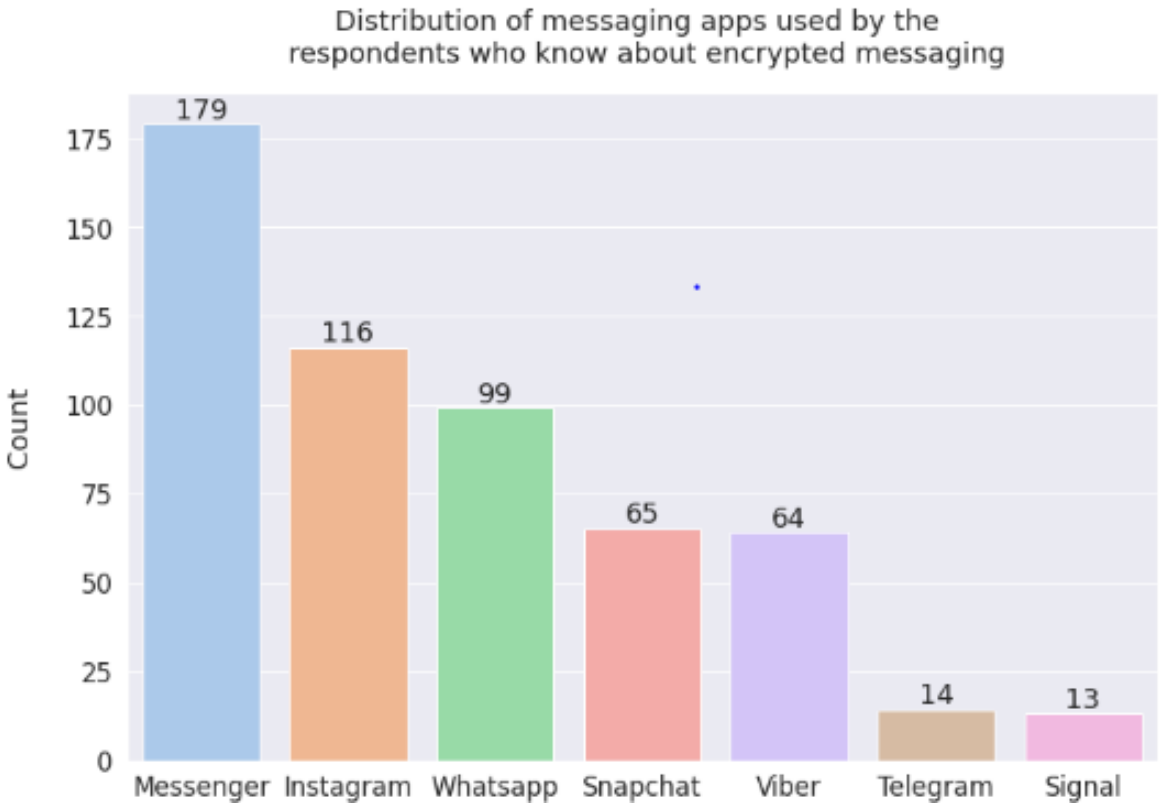

Figure 19: Distribution of messaging apps used by the respondents who don't know about encrypted messaging

Interestingly, a similar trend of using Messenger and Instagram was seen among the respondents who claimed to be knowledgeable about encrypted messaging. WhatsApp and Viber were the most popular encrypted apps while Telegram and Signal were the least popular.

4. User understanding of how their personal data is secured by social media platforms in accordance with the privacy policies they have accepted

a) Distribution of respondents who read ToC on SNS:

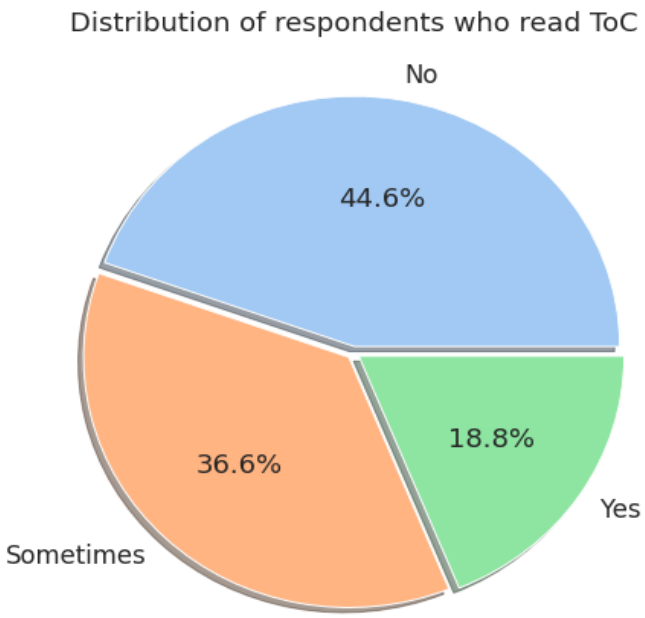

Figure 20: Distribution of respondents who read ToC on SNS

It can be seen that only 18.8% of our total respondents make it a habit of reading ToC on SNS, 36.6% only read them sometimes and 44.6% never read them. Reading habits could be influenced by multiple factors including accessibility, readability, and length of the documents. Lengthy ToCs could be a barrier for most users to read them thoroughly every time (Elks, 2012). But do privacy notices and conditions have to be very long in order to make users alert on privacy practices?

b) Relationship between the accessibility of Privacy Policies documents on SNS and the number of users reading them

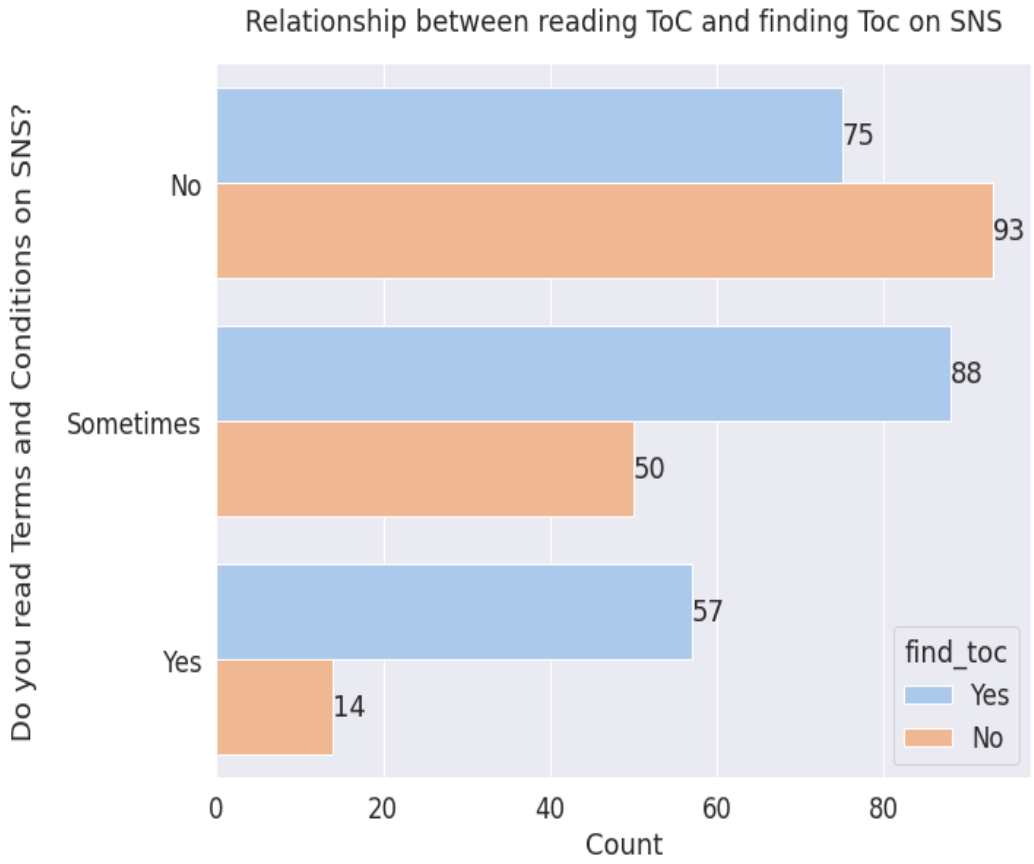

Figure 21: Relationship between reading ToC and finding ToC on SNS

It can be seen that, compared to people who regularly or sometimes read ToC on SNS, respondents who do not read them are not sure where to find these documents on the platforms. This could be because the documents are hard to locate on the SNS. As reported in research titled '(Un)informed Consent', users are more likely to interact with a privacy notice positioned on the lower left side of the screen in a computer screen and lower part of the mobile screen (Utz et al., 2019). Placement of the Privacy Policy banners might affect the user journey in finding the complete Privacy notices.

c) Awareness on digital footprints on SNS

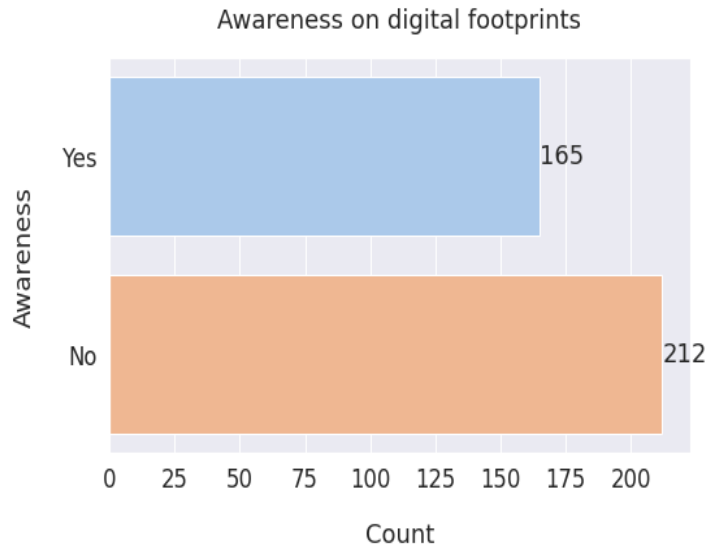

Figure 22: Awareness on digital footprints on SNS

Among our respondents, 43.8% were aware of their digital footprints on SNS while the rest 56.23% were not aware of what a digital footprint is.

d) Awareness of one's data online being used to target ads on SNS

Our survey explored whether our respondents were aware that their online activity data was being used to target ads on SNS or not. More than half of them (63.12%) were aware about this, and only 9.02% weren't aware about this. 27.85% were not so sure about this.

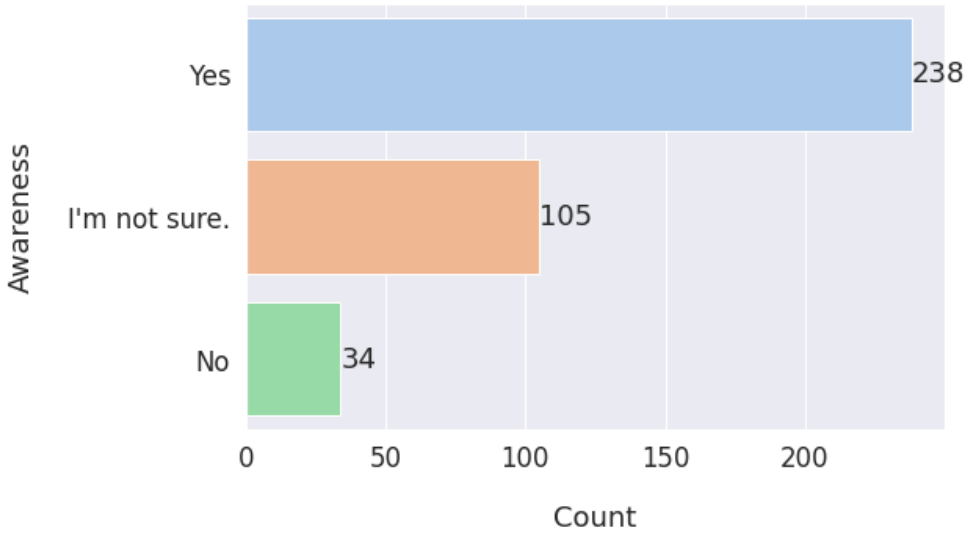

Figure 23: Awareness of one's data online being used to target ads on SNS

e) Frequency of getting targeted ads on SNS

65.78% of our respondents stated that they receive ads on SNS often or even always, while 13.8% of them reported having rarely or never received them. The remaining 20.42% reported having received them sometimes.

How often do you get targeted ads on SNS?	Number of participants
Always	29.71%
Often	36.07%
Sometimes	20.42%
Rarely	6.10%
Never	7.69%

Table 5: Frequency of getting targeted ads on SNS

f) Relevancy of ads presented to respondents on SNS

When asked about how relevant they feel the presented ads on SNS are, 30.22% gave a relevancy score of 3. 50.1% of our respondents gave a relevancy score of less than 3. And, only 19.68% gave a score above 3.

How relevant do you find those ads?	Number of participants
1	22.02%
2	28.12%
3	30.24%
4	13.00%
5	6.63%

Table 6: Relevancy of ads presented to respondents on SNS

g) Comfort of sharing personal information on SNS with third-party advertisers and respondents' habit of reading ToC on these platforms

With respondents who have no idea about the sharing of personal information on SNS with third-party advertisers, 30 out of 50 respondents responded that they do not read the ToC document on SNS. As these ToC documents are a one-stop page detailing third-party data usage, respondents who skip reading ToC might be unaware of such activities happening on SNS.

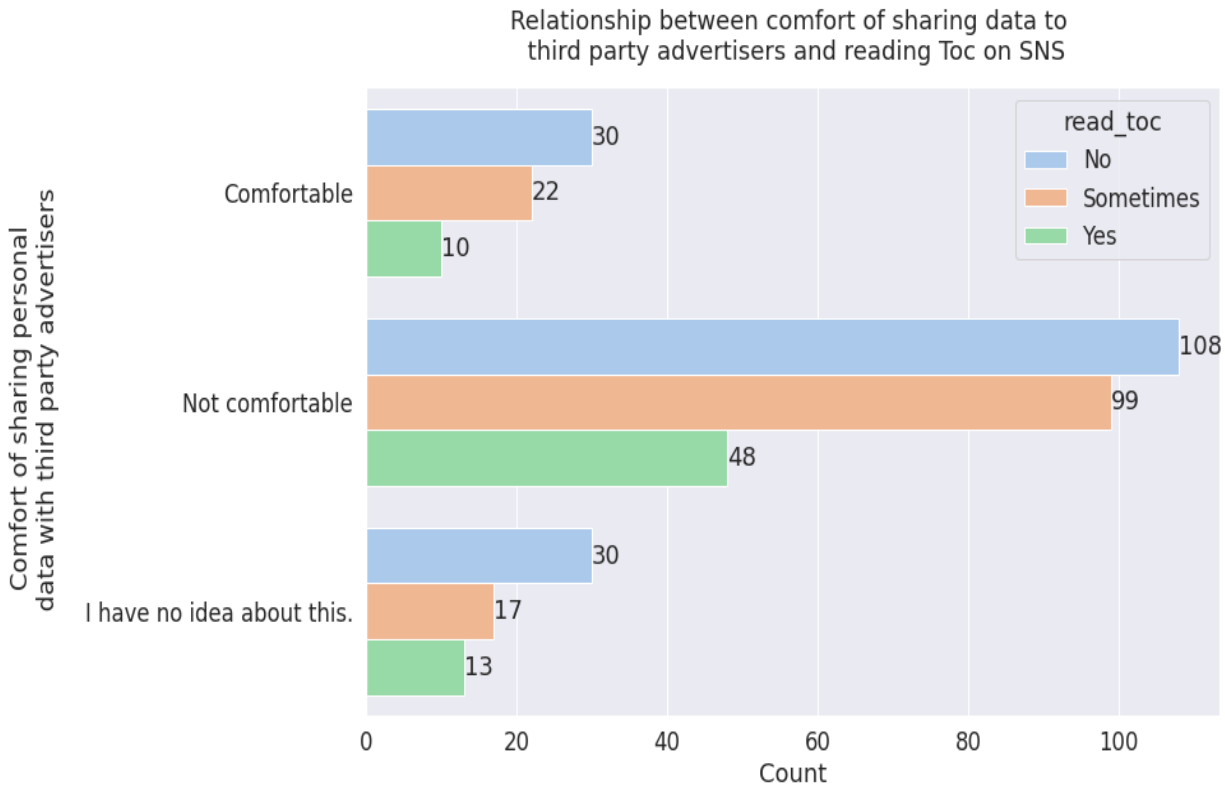

Figure 24: Comfort of sharing personal information on SNS with third-party advertisers and respondents' habit of reading ToC

h) Comfort of sharing deleted information on SNS with third-party advertisers and respondents' habit of reading ToC on these platforms

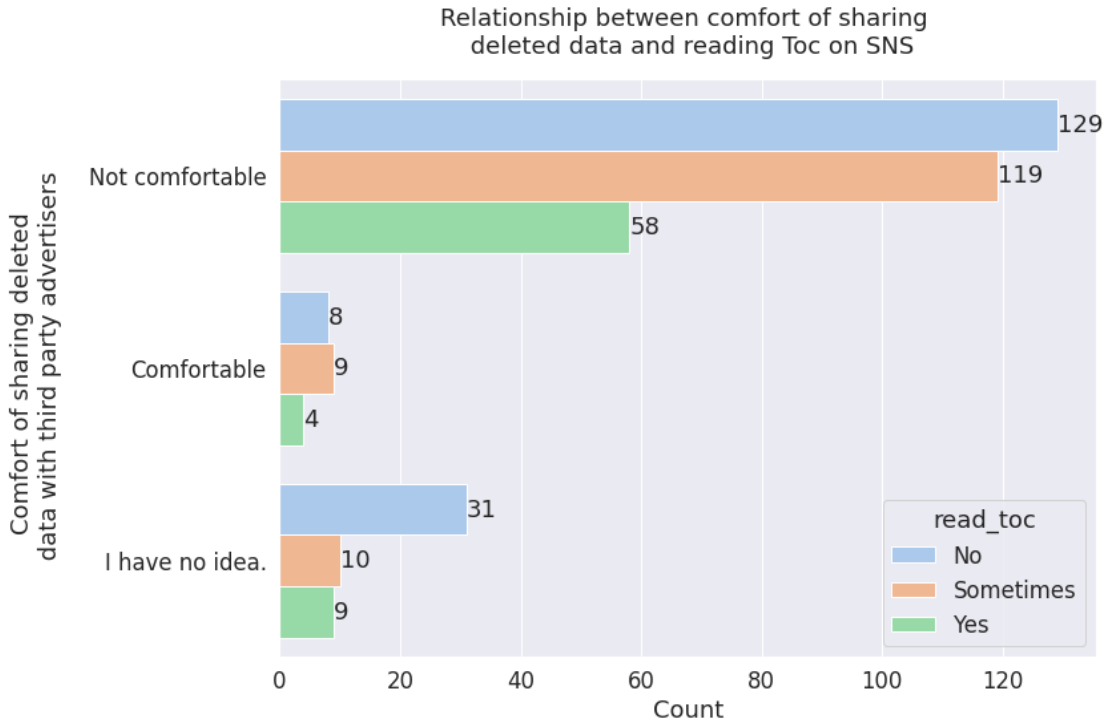

Figure 25: Comfort of sharing deleted information on SNS with third-party advertisers and respondents' habit of reading ToC

i. With respondents who have no idea about the access of their deleted data on SNS to third-party advertisers, 31 out of 50 respondents have not read the ToC document on SNS. As these policy documents on platforms like Facebook and Twitter detail the retention of deleted data among third parties, respondents who skip reading those documents might be unaware of their deleted data being retained and transmitted on SNS.

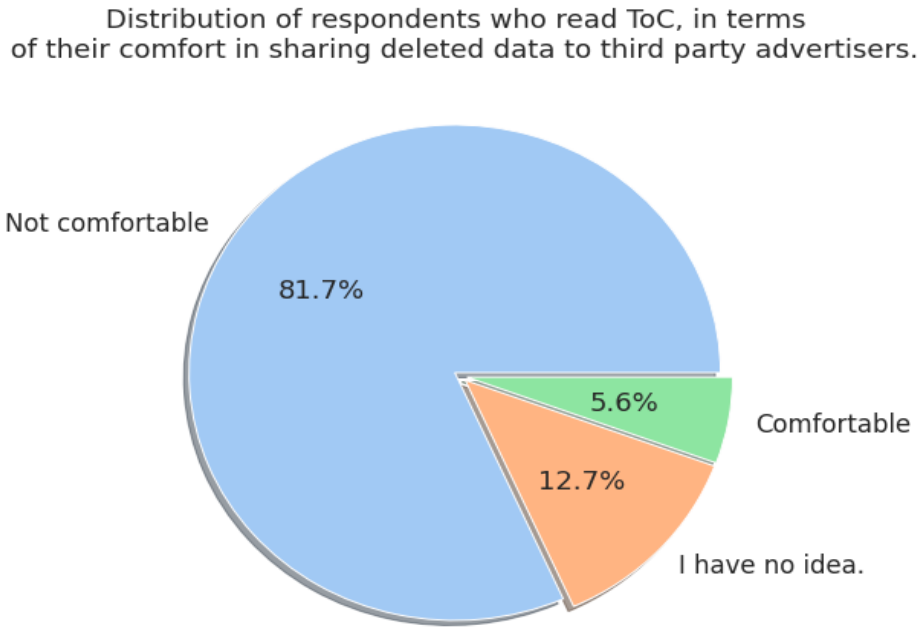

Figure 26: Distribution of respondents who read ToC, in terms of their comfort in sharing deleted data with third-party advertisers

ii. If we analyze the respondents who said they read the ToC of SNS, it can be seen that 81.7% of them are not comfortable sharing their deleted data with third-party advertisers. Interestingly, 5.6% of them still had no idea that their deleted content could still be accessed by third-party advertisers. This could be because of the lack of interpretability of the documentation language in the ToC or Privacy Policies documents.

A study on the design of privacy policies mentioned how these documents are hard to interpret because they are created without the needs of real users in mind (Waldman, A. E., 2018). Hence, if SNS platforms acknowledged the patterns of a user's disclosure decisions online and focused on simpler language translations alongside drafting legal language documents, the documents would be more interpretable to the public.

i) Privacy preferences of respondents who read ToC

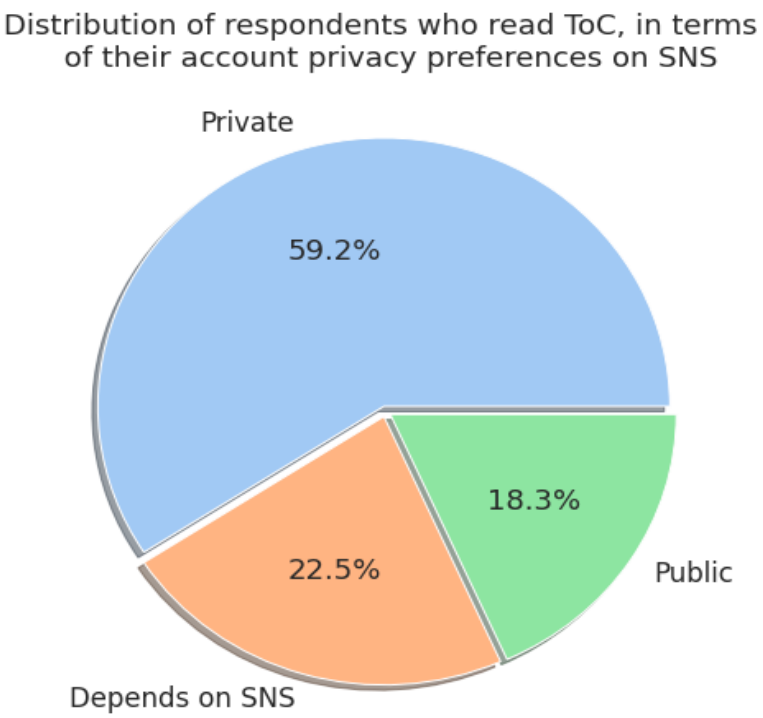

Figure 27: Distribution of respondents who read ToC, in terms of their account privacy preferences on SNS

Of the respondents who read ToC, more than half (59.2%) keep their social media accounts private. Although privacy preferences might depend on different attributes of the user as discussed in finding 1, it could also be impacted by their understanding of how their personal data is being used- all of which is mentioned in the ToC documents.

Conclusion

This research is one of the very few researches in Nepal to gather data from the respondents to study their engagement and privacy concerns on SNS. The survey questionnaire consisted of over thirty questions divided into three sections from social media engagement to privacy maintenance techniques. The survey's findings are summarized and compared with some existing international research papers, along with some of the more intriguing discoveries.

This sample of findings demonstrates that people favor private over public accounts and that their choice of a profile, information-sharing practices, and privacy preferences depend on a variety of criteria. Factors such as age, degree of privacy, type, and level of permission are discovered to be some of the deterministic variables. Respondents chose to maintain private accounts on Instagram and Facebook, where they post visual contents like photos and videos frequently. The results also show that people are typically willing to use their real names, and reveal personal information like their birth dates and hometowns, work, and education, but are hesitant to share their relationship status and check-ins. The kind of information or subject that they are sharing also seems to be influenced by the individual's characteristics. For instance, men and women who identify as cisgender, did not hesitate that much to sharing their gender information, compared to people with trans and gender diverse identities who chose not to. People are also reluctant to share their real locations possibly because of the concern that their whereabouts could be followed resulting in dangerous or unsafe situations. Even though the majority of people value privacy, very few people use anonymous identities on SNS, despite the apparent correlation between privacy and anonymity. As most of our respondents used SNS to communicate with their families, staying anonymous while doing so might become a barrier in interactions. Moreover, the majority of those who choose to remain anonymous do so for recreational purposes alone and have no strong privacy requirements.

A significant portion of respondents who are unaware of their user data and deleted data being shared with third-party advertisers have not read the ToC. Moreover, they find it difficult to locate the documents. Even among respondents who read these documents, some of them still had no idea about third-party access to their data, which could be because of a lack of interpretability of the documents. Readability and length of the T&C are also a concern for most people. With or without being informed about the privacy risks that come along with the use of social media, the majority of SNS users choose to skip policy documents like ToC and privacy policies. A lot of people are also aware of encrypted messaging but they still find it convenient to use Messenger or Instagram for messaging over highly encrypted apps like Telegram and Signal.

The findings from the research can be helpful in evaluating what factors influence privacy concerns, what kinds of information the general public is prepared to contribute and why, as well

as how well they understand privacy policies and personal data on SNS. Tech-makers can be mindful of what they are asking from users. For instance, if a field like a gender is not required, they should make it optional or eliminate it altogether. In case it is a compulsory field, they could add info boxes explaining where this field will be utilized. As for the general public, they can be aware of the things they are sharing, and how their information might be abused for impersonation, identity theft, and other illegal acts online. Considering the readability issues with policy documents on SNS, long documents could be broken up into manageable chunks which may encourage users to read privacy documents more frequently. If SNS platforms acknowledged patterns of a user's online disclosure decisions when drafting privacy notices and focused on simpler translations of the documents in legal language, it might help to make the documents much more comprehensible. Additionally, placing crucial documents on accessible pages on SNS would increase user engagement with such type of content.

Future work

In order to have a deeper understanding of privacy concerns among respondents, the research could be designed to acknowledge details about users' knowledge of privacy policies and application permissions. More qualitative questions could be added to the survey to find out how they view privacy as it is personal and subjective. Similarly, narrowing down the research to one or two SNS could be helpful to deduce profound insights. For a clearer understanding of how certain factors affect user privacy maintenance behavior online, mathematical techniques like correlation analysis can also be used.

References

Acquisti, A. and Gross, R. (2006) Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. Springer Berlin, Heidelberg, 36-58. http://dx.doi.org/10.1007/11957454_3

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. IEEE Security and Privacy Magazine, 3(1), 26–33. https://www.heinz.cmu.edu/~acquisti/papers/acquisti.pdf

Aljohani, M., Nisbet, A., & Blincoe, K. (2016). A survey of social media users privacy settings & information disclosure. https://ro.ecu.edu.au/ism/198/

Appel, G., Grewal, L., Hadi, R., & Stephen, A. T. (2020). The future of social media in marketing. *Journal of the Academy of Marketing Science*, *48*(1), 79-95. https://link.springer.com/article/10.1007/s11747-019-00695-1

Altman, I. (1975). The environment and social behavior: privacy, personal space, territory, and crowding. https://eric.ed.gov/?id=ed131515

Barnet, B., & Bossio, D. (2020, October 6). *Netflix's the social dilemma highlights the problem with social media, but what's the solution?* The Conversation. https://theconversation.com/netflixs-the-social-dilemma-highlights-the-problem-with-social-media-but-whats-the-solution-147351

Bhattacharya, K., Ghosh, A., Monsivais, D., Dunbar, R.I.M. & Kaski, K. (2016). Sex differences in social focus across the life cycle in humans. Royal Society Open Science, 3(4). https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4852646/

Bubas, G., Orehovacki, T. & Konecki, M. (2008). Factors and Predictors of Online Security and Privacy Behavior. Journal of Information and Organizational Sciences. 32. 79-98. https://www.bib.irb.hr/375517/download/375517.63-360-1-PB.pdf

Chopra, R., & Bareja, A. (2022, August 10). *Can privacy laws in Nepal protect its citizens from data breach?* S.S Rana & Co. https://ssrana.in/articles/privacy-laws-in-nepal-data-breach/

Çınar, N., & Ateş, S.(2022)." Data Privacy in Digital Advertising: Towards a Post Third-Party Cookie Era", in Filimowicz, M.(Ed.) Privacy: Algorithms and Society, Routledge. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4041963

Cohen, S. (2016). Privacy Risk with Social Media. HuffPost. https://www.huffpost.com/entry/privacy-risk-with-social_b_13006700

Donath, J. (2007). Signals in social supernets. *Journal of Computer-Mediated Communication*, *13*(1), 231-251. https://academic.oup.com/jcmc/article-abstract/13/1/231/4583064

Elks, S. (2012, December 4). Terms and conditions on websites can be 'longer than a Shakespeare play'. Metro. https://metro.co.uk/2012/03/22/terms-and-conditions-on-websites-can-be-longer-than-a-shakespeare-play-362520/

Gluck, J., Schaub, F., Friedman, A., Habib, H., Sadeh, N., Cranor, L. F., & Agarwal, Y. (2016). How short is too short? implications of length and framing on the effectiveness of

privacy notices. In Twelfth symposium on usable privacy and security (SOUPS 2016) (pp. 321-340). https://www.usenix.org/system/files/conference/soups2016/soups2016-paper-gluck.pdf

Hallinan, D., Friedewald, M., & McCarthy, P. (2012). Citizens' perceptions of data protection and privacy in Europe. *Computer law & security review*, *28*(3), 263-272. https://www.sciencedirect.com/science/article/abs/pii/S026736491200057X

Jones, K., Nurse, J. R., & Li, S. (2020, May). Behind the mask: A computational study of Anonymous' presence on Twitter. In *Proceedings of the International AAAI Conference on Web and Social Media* (Vol. 14, pp. 327-338). https://ojs.aaai.org/index.php/ICWSM/article/view/7303

Kaiser, A. F. (2016). Privacy and security perceptions between different age groups while searching online (Bachelor's thesis, University of Twente). https://essay.utwente.nl/70190/1/Kaiser_BA_BMS.pdf

Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. Business horizons, 53(1), 59-68. https://www.sciencedirect.com/science/article/abs/pii/S0007681309001232

Kemp, S. (2022, February 15). *Digital 2022: Nepal*. Data Reportal. https://datareportal.com/reports/digital-2022-nepal

Kemp, S. (2022, October 20). *Digital 2022: October Global Statshot Report*. Data Reportal. https://datareportal.com/reports/digital-2022-october-global-statshot

Lamberton, C., & Stephen, A. T. (2016). A thematic exploration of digital, social media, and mobile marketing research's evolution from 2000 to 2015 and an agenda for future research. Journal of Marketing, 80(6), 146–172. https://ora.ox.ac.uk/objects/uuid:f6995406-9460-40b8-8743-857c8610139a

Lee, H., Park, H., & Kim, J. (2013). Why do people share their context information on Social Network Services? A qualitative study and an experimental study on users' behavior of balancing perceived benefit and risk. International Journal of Human-Computer Studies, 71(9), 862–877. https://sci-hub.se/10.1016/j.ijhcs.2013.01.005

Levmore, S., & Nussbaum, M. C. (2012). *The offensive internet: Speech, privacy, and reputation* (p. 10). Harvard University Press. https://chicagounbound.uchicago.edu/book_chapters/708/

Litman-Navarro, K. (2019, June 12). *We read 150 privacy policies. They were an incomprehensible disaster*. The New York Times. https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html

O'Brien, K. (2012, February 5). *Austrian law student faces down Facebook*. The New York Times. https://www.nytimes.com/2012/02/06/technology/06iht-rawdata06.html

Pew Research Center. (2022, October 7). *Social media fact sheet*. Pew Research Center: Internet, Science & Tech. https://www.pewresearch.org/internet/fact-sheet/social-media/

Poddar, A., Mosteller, J., & Ellen, P. S. (2009). Consumers' rules of engagement in online information exchanges. *Journal of Consumer Affairs*, *43*(3), 419-448. https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1745-6606.2009.01147.x

Rodriguez, R. (2012). Privacy on Social Networks: Norms, Markets, and Natural Monopoly. In S. Levmore & M. C. Nussbaum (Eds.), *The offensive internet: Speech, privacy, and reputation* (p. 238). Harvard University Press. https://chicagounbound.uchicago.edu/book_chapters/708/

Sheehan, K. B. & Hoy, M. G. (2000). Dimensions of Privacy Concern Among Online Consumers. Journal of Public Policy & Marketing, 19(1), 62–73. https://www.jstor.org/stable/30000488

Stone, G. R. (2012). Privacy, the First Amendment and the Internet. In S. Levmore & M. C. Nussbaum (Eds.), *The offensive internet: Speech, privacy, and reputation* (pp.217-236). Harvard University Press. https://chicagounbound.uchicago.edu/book_chapters/708/

Stutzman, F., & Kramer-Duffield, J. (2010, April). Friends only: examining a privacy-enhancing behavior in facebook. In *Proceedings of the SIGCHI conference on human factors in computing systems* (pp. 1553-1562). https://dl.acm.org/doi/abs/10.1145/1753326.1753559

Ur, B., Leon, P. G., Cranor, L. F., Shay, R., & Wang, Y. (2012, July). Smart, useful, scary, creepy: perceptions of online behavioral advertising. In proceedings of the eighth symposium on usable privacy and security (pp. 1-15). https://dl.acm.org/doi/abs/10.1145/2335356.2335362

Utz, C., Degeling, M., Fahl, S., Schaub, F., & Holz, T. (2019). (Un)informed consent. Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security.. https://dl.acm.org/doi/abs/10.1145/3319535.3354212

Vincent, S. (2020, October 28). *Data privacy is a human right*. Human Rights Watch. https://www.hrw.org/news/2018/04/19/data-privacy-human-right?fbclid=IwAR3oqa6n5PJMOsmzqpRYWREPB2x9uD2ilL8aeBC-u8zGLJJAxnrnKhMNHTE

Wagner, D., Lopez, M., Doria, A. & Pavlyshak, I. (2010). Hide and seek: Location sharing practices with social media. 55-58. https://www.researchgate.net/publication/221270296_Hide_and_seek_Location_sharing_practices_with_social_media

Waldman, A. E. (2018). Privacy, notice, and design. Stan. Tech. L. Rev., 21, 74. https://digitalcommons.nyls.edu/cgi/viewcontent.cgi?article=2330&context=fac_articles_chapters

Westin, A. F. (1968). Privacy and Freedom (New York: Atheneum, 1968), p. 7. https://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=3659&context=wlulr

Appendix

Survey Questionnaire

General Information

1. Age
2. Which district are you from?
3. Gender Identity
    a. Cisgender Man
    b. Cisgender Woman
    c. Transgender Man
    d. Transgender Woman
    e. Non-binary/non-conforming
    f. Gender Fluid
    g. Prefer not to respond
    h. Custom
4. Sexual Orientation
    a. Heterosexual Man
    b. Heterosexual Woman
    c. Gay
    d. Lesbian
    e. Bisexual
    f. Pansexual
    g. Asexual
    h. Queer
    i. Prefer not to respond
    j. Custom
5. Do you identify as someone who has any form of physical disability?
    a. Yes
    b. No
6. Do you identify as someone who has any form of mental disability?
    a. Yes
    b. No
7. If you answered yes to any of the above two questions, please share with us the form of disability if you are comfortable with that.
8. Are you a student or a working professional?
    a. Student
    b. Working Professional

c. Both
d. Neither

9. Field of Study
10. Professional Field
11. Position
12. Company/Organization you work for

Social Media Usage and Engagement

13. How many social media apps are there on your phone?
14. How many hours per day do you spend on social media?
15. What social media apps do you use on a regular basis? Choose your top 3 social media apps.
    a. Facebook
    b. Instagram
    c. Twitter
    d. TikTok
    e. Reddit
    f. Pinterest
    g. LinkedIn
    h. YouTube
    i. Others
16. Why do you use social media? Choose all the options that apply.
    a. To post my life updates and thoughts on my private profile
    b. To connect with my family and friends
    c. To consume digital content online (news, products, opportunities, memes, etc.)
    d. To publish my creative works and do personal branding (news, informative content, memes, entertainment, etc.)
    e. To publish content on community pages/groups (news, informative content, memes, entertainment, etc.)
    f. I am a social media influencer. I make social media content as my career.
    g. To run my business page for outreach or sales
    h. Others
17. What kind of content do you mostly publish on social media? Choose all the options that apply.
    a. Textual content (Status/Tweet)
    b. Photos
    c. Videos
    d. Infographics (Textual as well as visual content combined)
    e. Livestreams

f. Links to external media sources (articles, games, products, etc.)

18. How often do you post on social media? This includes both posts and temporary content like stories that disappear within a fixed period of time like 24 hours.
    a. Very often (Daily)
    b. Often (1-4 times a week)
    c. Moderately (Once every month)
    d. Rarely (Once every few months)
    e. Very Rarely (Once a year or less)
19. Do you use messaging platforms online? If yes, which of the following messaging platforms do you use the most? Select up to 3 platforms you mostly use.
    a. I don't use any online messaging app.
    b. Messenger.
    c. Instagram Direct Messages.
    d. WhatsApp
    e. Viber
    f. Signal
    g. imo
    h. Snapchat
    i. Telegram
    j. The app that I use the most isn't on the list
    k. Other
20. Do you know about encrypted messaging online?
    a. Yes
    b. No

Privacy Maintenance Techniques on Social Media Platforms

21. Do you mostly prefer having your personal account, public or private on social media?
    a. Private
    b. Public
    c. Depends on the social media I am posting on
22. Tick all your personal social media accounts that are private.
    a. Facebook
    b. Instagram
    c. Twitter
    d. TikTok
    e. Reddit
    f. Pinterest
    g. LinkedIn

h. YouTube
i. None of the above

23. Tick all your personal social media accounts that are public.
    a. Facebook
    b. Instagram
    c. Twitter
    d. TikTok
    e. Reddit
    f. Pinterest
    g. LinkedIn
    h. YouTube
    i. None of the above
24. Have you ever used any anonymous account while interacting on social media?
    a. Yes, I actively interact with others using an anonymous account.
    b. Yes, but I do not actively interact with others using an anonymous account.
    c. No
25. If yes, what is/are the reasons behind being anonymous on social media platforms? Choose all the options that apply.
    a. I stay anonymous for no major reason; it is just for fun.
    b. I stay anonymous to keep my private information undisclosed.
    c. I stay anonymous to prevent others from tracking my social media activities.
    d. I stay anonymous because society would hesitate to accept my real identity.
26. Which of these fields are you not comfortable filling on social media? Choose all the fields that apply.
    a. Name
    b. Birthdate
    c. Gender
    d. Hometown
    e. Current town
    f. Education
    g. Work
    h. Relationship Status
    i. Interests/Hobbies
    j. Check-ins
    k. None
27. How often do you update your latest information on social media platforms?
    a. As soon as anything changes.
    b. Timely review my information if anything changes.
    c. Sometimes, randomly update whenever I feel like it.
    d. Rarely, update only if needed.

e. Never, I don't update information on social media.

28. How often do you add a real location, while posting pictures/videos?
    a. Always
    b. Occasionally when needed
    c. Never, I don't like adding location information.
29. How often do you revise and delete/hide your past posts/content?
    a. Never, I don't go through my past contents once I post them.
    b. I go through my past contents but I don't delete/hide them.
    c. I revise them frequently and delete or hide the ones I find embarrassing or irrelevant.
    d. I always delete content after a certain time of posting it.
30. How often do you filter your friend/followers list?
    a. Very often (Daily)
    b. Often (1-4 times a week)
    c. Moderately (Once every month)
    d. Rarely (Once every few months)
    e. Very rarely (Once a year or less)

Data Collection on Social Media Platforms

31. How often do you receive promotional messages, spam or calls from unknown numbers/ users/boots?
    a. Mostly
    b. Often
    c. Sometimes
    d. Rarely
    e. Never
32. How frequently are your approached by strangers on social media?
    a. Mostly
    b. Often
    c. Sometimes
    d. Rarely
    e. Never
33. How often do you come across targeted ads on social media platforms?
    a. Mostly
    b. Often
    c. Sometimes
    d. Rarely
    e. Never

34. On a scale of 1 to 5, how relevant do you find these ads?
35. How often do you find yourself filtering/hiding/skipping such ads?
    a. Mostly
    b. Often
    c. Sometimes
    d. Rarely
    e. Never
36. Do you know where to find privacy policies and terms and conditions for social media/messaging platforms?
    a. Yes
    b. No
    c. I have never checked privacy policies or terms and conditions.
37. Do you read the presented terms and conditions before signing up on a platform?
    a. Yes
    b. Sometimes
    c. No
38. Do you know what a digital footprint is?
    a. Yes
    b. No
39. Do you think that your information and activity on social media platforms is being used to suggest advertisements for you?
    a. Yes
    b. No
    c. I'm not sure.
40. How comfortable are you with third-party advertisers using your online data to suggest advertisements you see on your social media?
    a. I'm comfortable, I don't mind if they use my personal information.
    b. I'm comfortable because I find ads helpful.
    c. I'm not comfortable, but I can't stop them from using my data.
    d. I'm not comfortable at all.
    e. I have no idea about data and its use by the third-party advertisers.
41. Are you comfortable if a third party has access to your past data that you already deleted or archived?
    a. I'm comfortable, I don't mind if they use my deleted or archived personal information.
    b. I am comfortable as long as they don't misuse my deleted data.
    c. I'm not comfortable, but I can't stop them from using my data.
    d. I'm not comfortable at all.
    e. I have no idea about third-party advertisers having access of my deleted content.
42. Who referred this survey to you?

Deconstructing Online Privacy: Online User Engagement and Privacy Concerns on Social Media

NEPAL

SAFER-I

Safer-I is a campaign devoted to crafting a safer digital space for everyone. The ‘I’ in ‘Safer-I’ stands for Internet, Information, Inclusivity, and Individuality. Our work is primarily focused on crafting a safe, accessible, ethical, and inclusive digital space for everyone through hands-on workshops, advocacy, and social media awareness.

safer-i.org