PRIVACY PARADOX:
A STUDY AMONG THE YOUTH IN THIRUVANANTHAPURAM

A Dissertation submitted to the University of Kerala in partial fulfillment of the requirements for the Degree of MA Sociology

Submitted by

ALEN JOSE

Exam code: 56013405

Candidate code: 56017115001

Subject code: SO245

Department of Sociology
Loyola College of Social Science, Thiruvananthapuram

2017-2019

DECLARATION

I, **Alen Jose,** do here by declare that the dissertation titled **"PRIVACY PARADOX: A STUDY AMONG THE YOUTH IN THIRUVANANTHAPURAM"** is based on the original work carried out by me and submitted to the University of Kerala during the year 2017-2019 towards partial fulfillment of the requirements for the Master of Sociology Degree Examination. It has not been submitted for the award of any degree, diploma, fellowship or other similar title of recognition before.

Alen Jose

Thiruvananthapuram

Date: 23/9/2019

CERTIFICATE OF APPROVAL

This is to certify that the dissertation entitled **"**PRIVACY PARADOX: A STUDY AMONG THE YOUTH IN THIRUVANANTHAPURAM**"** is an authentic record of genuine work carried out by Mr. Alen Jose, fourth semester student of Master of Sociology under my supervision and guidance that is hereby approved for submission.

Prasad Ravikumar
Faculty, Dept. of Sociology
Loyola College of Social Sciences

Recommended for forwarding to the University of Kerala

Dr. Nisha Jolly Nelson
Head of the Dept. of Sociology
Loyola College of Social Sciences

Recommended for forwarding to the University of Kerala

Dr. Saji P Jacob
Principal
Loyola College of Social Sciences

Thiruvananthapuram
Date:-23/9/2019

Acknowledgement

I am indeed very happy to acknowledge the helping hands behind this research work. I am grateful to all the faculties of the department of sociology for adding me passion and interest for doing a research and for the contribution they had imparted through their classes and discussion. Especially, I render my sincere thanks to Dr. Nisha Jolly Nelson, head of the department for standing with all the support from the beginning of the research process.

I am also happy to remember the valuable support and encouragement from my classmates and batch mates. We had good discussions over the research that enhanced my vision regarding the procedure of the same.

I am grateful to Mr. R. Prasad, my research guide, who has been with my research work with suggestions.

With a deep sense of gratitude, I do remember the guidance and valuable suggestions of Dr. Saji P Jacob, my teacher and my principal, who stood with me in the bear some hours of the research. He was so kind to teach me the tough steps of the research with such patience.

Alen Jose

MA Sociology

Table of contents

List of Figures

Abstract

The concept of a "privacy paradox", initially formulated by Susan Barnes (2006) to define the perplexing divide between privacy-concerned adults and self-disclosing digital teenagers has evolved to incorporate discrepancies between individual attitudes and behavior when it comes to (online) privacy.

Review found that the issue of privacy online is itself not extensively researched, at least in comparison to other matters of public concern. As a relatively recent concept (the online aspect anyway), there is limited trend data available to track how public attitudes and actions on online data privacy have changed over the years. There are gaps in the evidence in terms of the views of different groups in society – including ethnic minority communities and disabled people. Meanwhile terminology is applied different across different studies; and much of the evidence is based on people's personal perceptions, rather than more objective measures. More and better evidence will be required in the future, to help inform our approach to these issues.

CHAPTER I

INTRODUCTION

Internet

The Internet is the decisive technology of the Information Age, and with the explosion of wireless communication in the early twenty-first century, we can say that humankind is now almost entirely connected, albeit with great levels of inequality in bandwidth, efficiency, and price.

People, companies, and institutions feel the depth of this technological change, but the speed and scope of the transformation has triggered all manner of utopian and dystopian perceptions that, when examined closely through methodologically rigorous empirical research, turn out not to be accurate. For instance, media often report that intense use of the Internet increases the risk of isolation, alienation, and withdrawal from society, but available evidence shows that the Internet neither isolates people nor reduces their sociability; it actually increases sociability, civic engagement, and the intensity of family and friendship relationships, in all cultures.

Our current "network society" is a product of the digital revolution and some major sociocultural changes. One of these is the rise of the "Me-centered society," marked by an increased focus on individual growth and a decline in community understood in terms of space, work, family, and ascription in general. But individuation does not mean isolation, or the end of community. Instead, social relationships are being reconstructed on the basis of individual interests, values, and projects. Community is formed through individuals' quests for like-minded people in a process that combines online interaction with offline interaction, cyberspace, and the local space.

Globally, time spent on social networking sites surpassed time spent on e-mail in November 2007, and the number of social networking users surpassed the number of e-mail users in July 2009. Today, social networking sites are the preferred platforms for all kinds of activities, both business and personal, and sociability has dramatically increased

— but it is a different kind of sociability. Most Facebook users visit the site daily, and they connect on multiple dimensions, but only on the dimensions they choose. The virtual life is becoming more social than the physical life, but it is less a virtual reality than a real virtuality, facilitating real-life work and urban living.

Because people are increasingly at ease in the Web's multidimensionality, marketers, government, and civil society are migrating massively to the networks people construct by themselves and for themselves. At root, social-networking entrepreneurs are really selling spaces in which people can freely and autonomously construct their lives. Sites that attempt to impede free communication are soon abandoned by many users in favor of friendlier and less restricted spaces.

Perhaps the most telling expression of this new freedom is the Internet's transformation of socio political practices. Messages no longer flow solely from the few to the many, with little interactivity. Now, messages also flow from the many to the many, multi-modally and interactively. By disinter mediating government and corporate control of communication; horizontal communication networks have created a new landscape of social and political change.

Networked social movements have been particularly active since 2010, notably in the Arab revolutions against dictatorships and the protests against the management of the financial crisis. Online and particularly wireless communication has helped social movements pose more of a challenge to state power.

The Internet and the Web constitute the technological infrastructure of the global network society, and the understanding of their logic is a key field of research. It is only scholarly research that will enable us to cut through the myths surrounding this digital communication technology that is already a second skin for young people, yet continues to feed the fears and the fantasies of those who are still in charge of a society that they barely understand.

Social Media

Information and communication technology has changed rapidly over the past 20 years with a key development being the emergence of social media.

The pace of change is accelerating. For example, the development of mobile technology has played an important role in shaping the impact of social media. Across the globe, mobile devices dominate in terms of total minutes spent online. This puts the means to connect anywhere, at any time on any device in everyone's hands.

Social media is being used in ways that shape politics, business, world culture, education, careers, innovation, and more.

A fascinating study by New York Times Consumer Insight Group revealed the motivations that participants cited for sharing information on social media. These include a desire to reveal valuable and entertaining content to others; to define themselves; to grow and nourish relationships and to get the word out about brands and causes they like or support.

- 84% - To support a cause or issues they feel strongly about.
- 94% - Share to pass valuable information. 49% of these respondents influence action about products by sharing.
- 68% - Use social sharing to build image and demonstrate who they are and what they stand for.
- 78% - To interact, grow, get a sense of fulfillment, nurture relationships and stay in touch with others.
- 69% - To participate and feel involved in things happening in the world.

These factors have caused social networks to evolve from being a handy means for keeping in touch with friends and family to being used in ways that have a real impact on society.

Social media is being used in ways that shape politics, business, world culture, education, careers, innovation, and more.

Here are seven ways the impact of social media is felt by individuals and social groups:

1. The Effect of Social Media on Politics - A new study from Pew Research claims that 62 percent of people get their news from social media, with 18 percent doing so very often.

   In comparison to other media, social media's influence in political campaigns has increased tremendously. Social networks play an increasingly important role in electoral politics — first in the ultimately unsuccessful candidacy of Howard Dean in 2003, and then in the election of the first African-American president in 2008.

   The New York Times reports that "The election of Donald J. Trump is perhaps the starkest illustration yet that across the planet, social networks are helping to fundamentally rewire human society." Because social media allows people to communicate with one another more freely, they are helping to create surprisingly influential social organizations among once-marginalized groups.

2. The Impact of Social Media on Society - Almost a quarter of the world's population is now on Facebook. In the USA nearly 80% of all internet users are on this platform. Because social networks feed off interactions among people, they become more powerful as they grow.

   Thanks to the internet, each person with marginal views can see that he's not alone. And when these people find one another via social media, they can do things — create memes, publications and entire online worlds that bolster their worldview, and then break into the mainstream.

   Without social media, social, ethical, environmental and political ills would have minimal visibility. Increased visibility of issues has shifted the balance of power from the hands of a few to the masses.

   The flipside: Social media is slowly killing real activism and replacing it with 'slacktivism'

   While social media activism brings an increased awareness about societal issues, questions remain as to whether this awareness is translating into real change.

Some argue that social sharing has encouraged people to use computers and mobile phones to express their concerns on social issues without actually having to engage actively with campaigns in real life. Their support is limited to pressing the 'Like' button or sharing content.

This is a very human reaction when people are given options that absolve them from responsibility to act. A 2013 study by the University of British Columbia's Sauder School of Business found that when people are presented with the option of 'liking' a social cause, they use this to opt out of actually committing time and money to a charitable cause. On the other hand, when people are allowed to show support in private, they are more likely to show meaningful support in terms of making a financial contribution.

The researchers found that a public endorsement is an action meant to satisfy others' opinions, whereas people who give in private do so because the cause is aligned to their values.

3. The Impact of Social Media on Commerce - The rise of social media means it's unusual to find an organization that does not reach its customers and prospects through one social media platform or another. Companies see the importance of using social media to connect with customers and build revenue.

   Businesses have realized they can use social media to generate insights, stimulate demand, and create targeted product offerings. This is important in traditional brick-and-motor businesses, and, obviously, in the world of e-commerce.

   Many studies suggest implementing social networks within the workplace can strengthen knowledge sharing. The result is to improve project management activities and enable the spread of specialized knowledge. Fully implementing social technologies in the workplace removes boundaries, eliminates silos, and can raise interaction and help create more highly skilled and knowledgeable workers.

   The flip side: Low number of social 'shares' can lead to negative social proof and destroy business credibility

   Interestingly, although the use of social sharing has become the norm rather than the exception in business, some companies, after experiencing first-hand some

negative effects of social media, have decided to go against the grain and remove the social sharing buttons from their websites.

A case study of Taloon.com, an e-commerce retailer from Finland, found that conversions rose by 11.9% when they removed share buttons from their product pages.

These results highlight the double-edged nature of the impact of social media. When products attract a lot of shares, it can reinforce sales. But when the reverse is true, customers begin to distrust the product and the company. This is what Dr. Paul Marsden, psychologist and author of 'The Social Commerce Handbook', referred to as 'social proof'.

4. The Effects of Social Media on the World of Work - Social media has had a profound effect on recruitment and hiring. 19 percent of hiring managers make their hiring decisions based on information found on social media. According to CareerBuilder's 2016 social media recruitment survey, 60 percent of employers use social networking sites to research job candidates.

   Professional social networks such as LinkedIn are important social media platforms for anyone looking to stand out in their profession. They allow people to create and market a personal brand.

5. The Impact of Social Media on Training and Development - Job candidates who develop skills on the latest and most advanced social media techniques are far more employable.

   A 2013 survey by Pearson Learning Solutions reported a significant increase in the use of social media in learning. Over half the educators who were interviewed agreed that social sharing encourages interaction, providing an environment that fosters learning.

   Blogs, wikis, LinkedIn, Twitter, Facebook, and podcasts are now common tools for learning in many educational institutions. Social media has contributed to the increase in long-distance online learning.

   Despite issues of lack of privacy and some instances of cheating among long-distance learners, this has not deterred social platforms from being used in education.

6. The Moral Challenges of Social Media

Social media has been blamed for promoting social ills such as:

a. Cyber bullying -Teenagers have a need to fit in, to be popular and to outdo others. This process was challenging long before the advent of social media. Add Facebook, Twitter, Snapchat and Instagram into the mix and you suddenly have teenagers being subjected feeling pressure to grow up too fast in an online world.

Michael Hamm, a researcher from the University of Alberta conducted a study that showed the effects of social media on bullying. 23% of teens report being targeted and 15 percent said they'd bullied someone on social media. Teenagers can misuse social media platforms to spread rumors, share videos aimed at destroying reputations and to blackmail others.

b. Lack of Privacy - Stalking, identity theft, personal attacks, and misuse of information are some of the threats faced by the users of social media. Most of the time, the users themselves are to blame as they end up sharing content that should not be in the public eye. The confusion arises from a lack of understanding of how the private and public elements of an online profile actually work.

Unfortunately, by the time private content is deleted, it's usually too late and can cause problems in people's personal and professional lives.

7. The Impact of Social Media on Personal Relationships - One of the effects of social media is encouraging people to form and cherish artificial bonds over actual friendships. The term 'friend' as used on social media lacks the intimacy identified with conventional friendships, where people actually know each other, want to talk to each other, have an intimate bond and frequently interact face to face.

Social Media Popularity

Some of the key takeaways from their Global Digital Report 2019 include:

- The number of internet users worldwide in 2019 is 4.388 billion, up 9.1% year-on-year.
- The number of social media users worldwide in 2019 is 3.484 billion, up 9% year-on-year.
- The number of mobile phone users in 2019 is 5.112 billion, up 2% year-on-year.

Annual growth continues apace, especially in active mobile social users - 42% penetration up 3% from 2018.

Share of web traffic by device highly favours mobile at 52% (staying stable year-on-year), whilst Desktop remains in second place with only 43% of device share to all web pages.

Northern, Western and South Europe and North America have the largest internet penetration with between 88%-95% internet users compared to the total population. Of these, South Europe has seen the biggest increase in internet penetration, with a year-on-year increase of 11%.

The global increase in social media usage since January 2018 is 9%. Saudi Arabia has the largest social media penetration in 2019 at 99%, which is well above the global average of 45%. Other countries with the largest social media penetration include Taiwan, South Korea and Singapore. Ghana, Kenya and Nigeria have the lowest levels of social media penetration.

Social Media Statistics

It is a fact of the internet that every click, every view and every sign-up is recorded somewhere.

Depending on your view, this is either very creepy or fantastically interesting.

There are all sorts of interesting stats about social media platforms and users.

For the curious, these represent a series of numbers that boggle the mind, users counted in tens and hundreds of millions, and time in millions and billions of hours. For marketers, knowing the statistics behind the social networks can inform strategy and spend, allowing focused targeting of users.

Social Media Statistics

- For context, as of January 2019, total worldwide population is 7.7 billion.
- The internet has 4.2 billion users.
- There are 3.397 billion active social media users.
- On average, people have 5.54 social media accounts.
- The average daily time spent on social is 116 minutes a day.
- 91% of retail brands use 2 or more social media channels.
- 81% of all small and medium businesses use some kind of social platform.
- Internet users have an average of 7.6 social media accounts.
- Social media users grew by 320 million between Sep 2017 and Oct 2018.
- That works out at a new social media user every 10 seconds.
- Facebook Messenger and Whatsapp handle 60 billion messages a day.
- When asked 81% of teenagers felt social media has a positive effect on their lives.

User Numbers

- 4Chan: 22 million
- Airbnb: 150 million users
- Facebook: 2.320 billion users
- Flickr: 90 million users
- Google+: 111 million users (RIP)
- Instagram: 1bn users
- LinkedIn: 610 million users
- MySpace: 15 million users
- Periscope: 10 million users

- Pinterest: 250 million users
- Reddit: 542 million users
- Snapchat: 186 million daily users
- Twitter: 326 million users
- Wechat: 1.12 billion users
- Weibo: 600 million users
- WhatsApp: 900 million users
- Youtube: 1.5 billion users

Social Media Business Statistics

- Social networks earned an estimated $8.3 billion from advertising in 2015
- $40bn was spent on social network advertising in 2016
- 38% of organizations plan to spend more than 20% of their total advertising budgets on social media channels in 2015, up from 13% a year ago
- Only 20 Fortune 500 companies actually engage with their customers on Facebook, while 83% have a presence on Twitter
- People aged 55-64 are more than twice as likely to engage with branded content than those 28 or younger
- 96% of the people that discuss brands online do not follow those brands' owned profiles
- 78 percent of people who complain to a brand via Twitter expect a response within an hour

Social Video Statistics

- Facebook now sees 8 billion average daily video views from 500 million users
- Snapchat users also sees 8 billion average daily video views

- US adults spend an average of 1 hour, 16 minutes each day watching video on digital devices
- Also in the US, there were 175.4m people watching digital video content
- 78% of people watch online videos every week, 55% watch every day
- It's estimated that video will account for 74% of all online traffic in 2017

Content Statistics

- On WordPress alone, 74.7 million blog posts are published every month
- A 2011 study by AOL/Nielsen showed that 27 million pieces of content were shared every day, and today 3.2 billion images are shared each day
- The top 3 content marketing tactics are social media content (83%), blogs (80%), and email newsletters (77%)
- 89% of B2B marketers use content marketing strategies

Google Statistics

- Google processes 100 billion searches a month
- That's an average of 40,000 search queries every second
- 91.47% of all internet searches are carried out by Google
- Those searches are carried out by 1.17 billion unique users
- Every day, 15% of that day's queries have never been asked before
- Google has answered 450 billion unique queries since 2003
- 60% of Google's searches come from mobile devices
- By 2014, Google had indexed over 130,000,000,000,000 (130 trillion) web pages
- To carry out all these searches, Google's data centre uses 0.01% of worldwide electricity, although it hopes to cut its energy use by 15% using AI

Facebook Statistics

- Facebook adds 500,000 new users every day; 6 new profiles every second
- 68% of all Americans are on Facebook
- 79% of all online US adults use Facebook
- 76% of Facebook users check it every day
- The average user spends 35 minutes on Facebook a day
- The average (mean) number of friends is 155
- Half of internet users who do not use Facebook themselves live with someone who does
- Of those, 24% say that they look at posts or photos on that person's account
- There are an estimated 270 million fake Facebook profiles
- The most popular page is Facebook's main page with 204.7m likes. The most liked non-Facebook owned page is Christiano Ronaldo's with 122.6m.
- There are 60 million active business pages on Facebook
- Facebook has 5 million active advertisers on the platform.
- Facebook accounts for 53.1% of social logins made by consumers to sign into the apps and websites of publishers and brands

Twitter Statistics

- 500 million people visit Twitter each month without logging in
- There is a total of 1.3 billion accounts, with 326 million monthly active users
- Of those, 44% made an account and left before ever sending a Tweet
- The average Twitter user has 707 followers
- But 391 million accounts have no followers at all
- There are 500 million Tweets sent each day. That's 6,000 Tweets every second
- Twitter's top 5 markets (countries) account for 50% of all Tweets
- It took 3 years, 2 months and 1 day to go from the first Tweet to the billionth
- 45% of Americans use Twitter

- 65.8% of US companies with 100+ employees use Twitter for marketing
- 77% of Twitter users feel more positive about a brand when their Tweet has been replied to

YouTube Statistics

- 300 hours of video are uploaded to Youtube every minute
- People now watch 1 billion hours of YouTube videos every day
- The average person wtaches 40 minutes of YouTube content a day
- More than half of YouTube views come from mobile devices
- 94% of American 18-24 year olds use YouTube
- The average mobile viewing session lasts more than 40 minutes
- The user submitted video with the most views is the video for Luis Fonsi's song 'Despacito' with 4.36 billion views
- YouTube sees around 1,148bn mobile video views per day
- In 2014, the most searched term was music. The second was Minecraft
- 9% of U.S small businesses use Youtube
- You can navigate YouTube in a total of 76 different languages (covering 95% of the Internet population)

Instagram Statistics

- There are 800 million Monthly Active Users on Instagram
- Over 95 million photos are uploaded each day
- There are 4.2 billion Instagram Likes per day
- More than 40 billion photos have been shared so far
- The average Instagram user spends 15 minutes a day on the app
- 90 percent of Instagram users are younger than 35
- When Instagram introduced videos, more than 5 million were shared in 24 hours

- Pizza is the most popular Instagrammed food, behind sushi and steak
- The most liked picture on Instagram is one of an egg
- 71% of Americans now use the platform
- 24% of US teens cite Instagram as their favorite social network

Pinterest Statistics

- Pinterest has 200 million active users each month
- 31% of all online US citizens use the platform
- 67% of Pinterest users are under 40-years-old
- The best time to Pin is Saturday from 8pm-11pm
- In 2014, male audience grew 41% and their average time spent on Pinterest tripled to more than 75 minutes per visitor

LinkedIn Statistics

- LinkedIn has 500 million members
- 106 million of those access the site on a monthly basis
- More than 1 million members have published content on LinkedIn
- The average CEO has 930 LinkedIn connections
- Over 3 million companies have created LinkedIn accounts
- But only 17% of US small businesses use LinkedIn

Snapchat Statistics

- Snapchat has 187m active daily users
- 60% of them are under 25
- In 2016, $90m was spent on Snapchat ads
- The average user spends 25 minutes a day on Snapchat

- 78% of American 18-24 year olds use the platform
- 47% of US teens think it's better than Facebook, while 24% think it's better than Instagram

Social Media and Privacy

Privacy is something we all value, but some value it more than others.

Social media has taken previously private conversations from offline to online. Facebook and Twitter have lead this charge onto an open and social web that reveals everything for all to see.

Add a little bit of youth, inexperience and lack of self-control and you have a feast of public communication in all its multimedia glory that sometimes makes you feel like a peeping tom.

To others it's a voyeur's paradise that compels and draws you back to view and read whether you like it or not.

The devices, technology and communication is changing rapidly but we as humans change slowly and adapting to this social network ecosystem is exposing our crawling adaptation to this new communication paradigm.

Research shows that nearly two thirds of us don't trust online companies like Facebook. Facebook has constantly tweaked its complex security settings over the years and despite protests and public outcry it seems that the situation has not improved. Studies show that 68% of Facebook users do not understand the social network's privacy settings.

According to a 2011 report by MSNBC and the Ponemon Institute internet users feel they have less control over their personal information today than they did 5 years ago.

Social media is here to stay, and with each passing day, it plays a greater role in our lives. That's why privacy on social media has never been more important. The way you use Twitter, Facebook, LinkedIn and the other social networks can have major impacts on your life, good or bad.

With a little bit of knowledge and a small dose of caution, however, you can enjoy all the benefits of social media with few of the risks. Here are some privacy concerns you should watch out for.

1. Account hacking and impersonation

Increasingly, spammers, hackers and other online criminals are targeting social networks. A compromised social media account makes for an appealing target: if they can get into your Facebook or Twitter account, they can impersonate you.

Why are they interested in your social media accounts? Because it's a much more effective way to spread viruses, malware, and scams than more traditional email spam. People tend to trust messages they get from their social media friends. They are more likely to click links without thinking twice, which can then infect their computers.

Even worse than malware is when cybercriminals use social media for identity theft. Our private social profiles contain a wealth of personal information, which can be leveraged to open credit card accounts in your name or otherwise abuse your digital identity.

2. Stalking and harassment

Not all social media privacy threats come from strangers. Sometimes, people in your life turn out to be less than friendly. Online stalking and cyberbullying have become very well-known threats, and social media makes them very easy to perpetrate.

In one recent incident, a woman who broke up with her boyfriend was horrified to discover some time afterward that he had broken into her Instagram account and posted transcripts of private messages about their relationship and other personal information. He also changed the account password so she couldn't log back in,

shared the information on other social networks, and then accused her of spreading it herself.

By the time she was able to access her accounts, thousands of friends, acquaintances, and professional contacts had seen her private information. It was a privacy nightmare on multiple levels. She had never given out her password to the ex, so he gained access by hacking her accounts or guessing her password.

3. Being compelled to turn over passwords

Unfortunately, there are situations where you may be asked to turn over access to your social media accounts. One of the most common is upon starting a new job. There has been a growing trend toward employers asking for access to social media accounts, to ensure that employees aren't sharing confidential information or trade secrets.

There have been a number of efforts at the state level to prevent companies from requesting this information. In 2016 alone, there were 39 state bills targeting this behavior. Unfortunately, the vast majority of them have failed.

Hopefully this trend will soon reverse. As people increase the amount of information they share on social media websites, the need for heightened security and privacy controls also increases. The potential for abuses and privacy violations is just too high when employers have access to an individual's social media accounts.

4. Walking a fine line between effective marketing and privacy intrusion

The debate over whether social media advertising works is over. Advertisers pumped billions of dollars into social media ads last year, and with all that investment comes the desire to target users more accurately.

Unfortunately, there is a dark side to all of this targeting. Already, Facebook has faced criticism over its ad targeting engine, which in some cases was illegally discriminating against certain types of people.

Facebook and other social media companies are trying to adapt, but there are conflicting interests between serving their paying advertising customers and their social media users. Balancing the needs of both is difficult to do, even when there isn't a financial incentive in place. As a result, it is likely that we will continue to see increased attempts at information gathering and privacy intrusions for the purposes of targeted marketing.

5. The privacy downside of location-based services

Most of today's social media users don't access the services on a traditional computer, they do it on their smartphones. As social media continues to take advantage of mobile devices and location-based services, the potential for privacy and security threats increases. In fact, most people's smartphones automatically collect location data continuously, and social media apps are some of the heaviest users of this data.

Without the guidance of fine-tuned legislation and privacy laws, social media services have a lot of leeway for how they use this data. There are more than a few examples of people being targeted by thieves or stalkers due to geo-location data automatically shared by their social media apps. After all, what more could a burglar ask for than to know when you're on vacation, far away from your home?

STATEMENT OF THE PROBLEM

Being anonymous – "the state of being not identifiable within a set of subjects" – is one of the features that the Internet provides. A user holds the privilege not to expose his/her personal details. Online privacy is defined as "an individual's ability to determine when, how, and to what extent personal information is disseminated to others in the virtual environment". Much like in real life, online anonymity is a feature supposed to ensure an individual's ability to keep and protect his/her identity.

However, it seems that the Internet, which enables users to exercise their online preferences, at the same time allows service providers and other users to collect their personal information, in many cases without consent. Thus, users are constantly faced with a dilemma: whether to choose online privacy over personalization, usability and interactivity.

This mismatch between users' online privacy attitudes and their actual behavior, when they prefer to utilize the comfort of the Internet at the expense of privacy and anonymity protection, was termed the "Privacy Paradox".

The privacy paradox describes an inconsistency between the concerns of people regarding privacy and their actual behaviour. This inconsistency still exists, but it can be well explained. In fact, there are many explanations. It should not be considered a paradox anymore. It's maybe more of a privacy dilemma, because people would like to do more but they also want to use services that would not exist without sharing their data.

The value of data is difficult to define. There is no equivalent of a stock-market for personal information. On top of it, the value is fluid. From an economic point of view, it is higher when a data-set is combined with other data, which means — on a functional level — the value of data increases if Google or Facebook have it. Also, if you share information now it will be on the internet for a long time. It is hard to predict what a data

set from 2018 is worth in 2022, taking into account the speed and the progress that the tech industry has made in the last decade.

The traditional understanding of privacy was very much connected to a physical space, like a house. If someone looked through your window people would have considered that a violation of privacy. What people did in their homes was private. If they did the same thing outside, in public, that was a different thing.

Cyberspace is completely different from that understanding. With the internet we lost a concept of space that defined a playing field for activities that we wanted to keep for ourselves. As soon as you connect to the internet, you are public.

Companies collect personal information. This happened because there was not enough time to react. The companies were moving very fast. Facebook became an internet giant in only ten years. It was just too fast for people to understand the risks and for governments to regulate the companies. It took the EU commission years to draft an update of the data protection regulation.

The legal system is just very slow and people are also very slow in understanding the implications of something like sharing personal information. The regulators needed to move much faster and the laws needed to be far more flexible and updated more often to keep up with the speed of tech companies.

SIGNIFICANCE OF THE STUDY

The indifference for data privacy at Facebook recently has resulted in revelations that various organizations collects user data for targeted advertising, particularly political advertising, to apparent success. While the most well-known offender is Cambridge Analytica, other companies have likely used similar tactics to collect personal data of Facebook users.

Researchers associated with Cambridge University, claimed in a paper that it "can be used to automatically and accurately predict a range of highly sensitive personal attributes including: sexual orientation, ethnicity, religious and political views,

personality traits, intelligence, happiness, use of addictive substances, parental separation, age, and gender,".

As privacy concerns multiply, there is little evidence that social networks are losing members. For all the concern that people express about their personal information, study of actual marketplace behavior suggest that people are not concerned in the protection of their own data profiles.

This study sheds light on the factors that influence this Paradox.

In the western world privacy is considered a human right. It seems evident that we see high concerns for privacy issues in countries that have a tradition of strong civil rights movements.

The debate has many parallels to the ecological movement. It has a tendency to position an individual in a bigger context, and it is about preserving a space for future generations. This could be an explanation for why we see higher concern in Germany. Germans see privacy as a risk not only for themselves as individuals, but as a threat for society and democracy.

And when people get concerned, media covers the story, people become more concerned and so on.

While the fight for privacy is an ongoing battle in the Western hemisphere, India seems not So much into it. There has been amendments in 2011 in reference to Privacy laws in India. But this came at a time when most of the citizens weren't that aware of their Internet Privacy Laws.

But the Internet game has changed when Mukesh Ambani entered telecommunications field with Jio with "free" and cheap Internet data plans. Almost five years have passed and the Internet users are growing.

India's internet users expected to register double digit growth to reach 627 million in 2019, driven by rapid internet growth in rural areas, market research agency Kantar IMRB Wednesday said.

Internet usage in the country has exceeded half a billion people for first time, pegged at 566 million, driven by rural internet growth and usage.

In its ICUBE 2018 report that tracks digital adoption and usage trends in India, it noted that the number of internet users in India has registered an annual growth of 18 percent and is estimated at 566 million as of December 2018, a 40 percent overall internet penetration it observed.

It projected a double digit growth for 2019 and estimates that the number of internet users will reach 627 million by the end of this year.

The situation has changed now. People have entered the Internet space without much knowledge of the Internet. On an average, 35,636 records were compromised in a data breach in India that ranked 15th in terms of total cost of breach.

"With organisations facing the loss or theft of over 11.7 billion records in the past three years alone, companies need to be aware of the full financial impact that a data breach can have on their bottom line - and focus on how they can reduce these costs," Mr. Whitmore said.

This is just the case for major corporate companies. So we can speculate how bad the scene is for normal Indian citizens. In 2016, BBC listed Truecaller as one of those platforms that are not safe as it would ask users to upload their phone's contact lists when they install them. Prior to 2016, in 2013 Truecaller was in the news after it admitted that it had fallen victim to a cyber-attack and suffered a data breach. However, it stayed to its point that no sensitive information had been exposed. These are not the only instances, the contact details collecting app again came under the interrogation light in 2017 in India when the Jio suffered a data leak.

The major question here is — even after witnessing so much, why people are still willing to install apps like Truecaller and hand over their contact details?

The Data (Privacy and Protection Bill), 2017 is the latest privacy bill awaiting amendment in India. This is for the further implementation of Aadhaar, which is another Privacy time bomb awaiting to happen.

Even if this is all happening, there hasn't been any widespread public concern about the data leakages in the media or public. There hasn't been much social researches regarding the privacy issues in India. A country where privacy is held very close to the heart, this kind of behavior is peculiar at most.

Secret services and anything that is related to governments can get controlled, at least in democratic countries. Also, tech companies can be regulated, as it happens now in the EU with the GDPR. Therefore, cyber-crime is the biggest challenge that we are facing. Another significant risk occurs when government agencies and tech companies do not keep their roles distinct. We have seen companies and secret services working hand in hand already and that is not a good sign.

Keeping all the above information in mind, the Privacy Paradox in the Indian subcontinent need to investigated and studied.

CHAPTER II

REVIEW OF LITERATURE

Modern information technologies grant us great power to broadcast our personal information to the world, but afford us much less control on how that information, once disseminated, will be used. Poorly thought emails, sent to an acquaintance in the heat of the moment, are forwarded to others causing embarrassment and regret; raunchy photos uploaded to a supposedly private network are made public; sensitive data privately revealed to companies are breached and stolen. And yet, most of us, lost in the immediately gratifying control over twits, blogs, and status updates, seem to spend little attention to the relative lack of control upon the longer term, yet more tangible consequences of our public disclosures. We even react in seemingly contradictory manners, when we feel that our right to decide what information should be disseminated, and how, has been violated. We do so, regardless of the objective privacy (or lack thereof) of that information: Many online social networks users compulsively compile and update detailed personal profiles, revealing plenty of private and even sometimes embarrassing information; however, how would they react if the same information they willingly disclosed had been published by another party?

With the emergence of web applications that enabled user-generated content and social interactions, the Web became a place where people can engage in a number of new activities. With the success of smart enabled devices people now actively share their data through various applications. However, the information about people, is often shared without their knowledge or consent. Due to this new privacy concerns arise, as the actual affordances of their data are far greater than people are even aware of. Regardless of the numerous controversies around privacy, people keep on sharing their data on the Web. However, privacy systems themselves (and the ways in which individuals express their preferences) have changed very little.

Privacy concerns an individual's ability to control what personal information is disclosed, to whom, when and under what circumstances. The unauthorized disclosure of personal information is normally considered a breach of privacy, although authorization and what is personal information are matters of dispute, particularly in an online context. Altman (1975, 18) describes privacy succinctly as "selective control of access to the self" although this might go beyond legal definitions and hark back to related definitions of privacy focused on the right to be left alone, as framed by Warren and Brandeis (1890).

The concept of a "privacy paradox", initially formulated by Susan Barnes (2006) to define the perplexing divide between privacy-concerned adults and self-disclosing digital teenagers, has evolved to incorporate discrepancies between individual attitudes and behavior when it comes to (online) privacy (Tufekci, 2008).

Recent revelations, such as Edward Snowden's release of secret information on the PRISM program, have led many Internet users to question their ability to effectively control the spread and use of personal data on the Internet (PEW Research, 2014). According to public perception, intelligence agencies – supported by large Internet service providers – are able to collect and analyze sensitive information about citizens to an unprecedented degree. As a result, Internet users express significant privacy concerns.

At the same time, a number of studies have found that Internet users only sparingly engage in privacy protection behavior, e.g., by restricting online privacy settings or deleting cookies – an apparent discrepancy between attitudes and actual behavior that has led some to declare a "privacy paradox" (Acquisti, 2004; Lanier & Saini, 2008).

If you have ever absentmindedly clicked 'accept' on terms and conditions without reading, reused the same password across multiple sites or gone months before checking your privacy settings, you are not alone. At the same time, you may also be part of the nearly three quarters of people in the UK who are concerned about their online privacy.

While this apparent disconnect between our attitudes and actions is not unique to data privacy, it becomes increasingly clear with every passing week that our ability to make informed decisions about our data is an issue that is worthy of greater consideration.

With Facebook's Cambridge Analytica scandal and the implementation of GDPR legislation, there's been a marked increase in focus this year on global privacy and the regulatory landscape. The question of how we define, value and better protect our privacy in the digital age has arguably never been a more significant and complex challenge.

Over the last 10 months, we've been working with leading research firm Ipsos MORI to analyse 50 pieces of evidence published within the last three years on citizens' attitudes and behaviours towards online privacy in the UK, including data from public, private and academic institutions.

While our analysis of the available research shows that most people do care about privacy online, many of us fail to take the necessary steps to better protect our personal data. This may be because we don't know how to, choose not to, are not fully aware of the possible risks, or feel powerless to do so. The mismatch between attitude and action has been coined by researchers as the 'Privacy Paradox'.

The evidence highlights some important issues that require further exploration. For example, people generally say they are more comfortable sharing data with public sector organizations than private companies – but how does this play out in practice? Do we genuinely have the desire or opportunity to regulate our interactions with companies in line with these attitudes; and how do public bodies build on this apparent trust in order to make the best use of data for public good, while effectively mitigating the risks?

There are also important variations between demographic groups. Younger people appear to be more privacy conscious than older people in many scenarios – but in other contexts the opposite is true. Meanwhile people from more deprived backgrounds appear more likely to be exposed to privacy risk than more affluent households. This raises a question of how people are supported to develop the necessary skills and confidence to navigate privacy considerations online, and whether this support is appropriately tailored to the needs of different groups.

The research also investigated data trade-offs. Many online products and services can be accessed in exchange for data about our behaviour or interests. Unsurprisingly the evidence shows that people in the UK make numerous such trade-offs for their data,

including for access to free or discounted products or services, a better more personalised service or simply through lack of an alternative.

But the price of access to the online world is not always free and the cost is not always obvious. As the 'old' saying goes – if the product is free, then you are the product. However the story isn't always quite as one-dimensional as headlines can often present it. Data trade-offs are made by people for a variety of reasons beyond purely personal gain, including for example allowing access to our data to support action in the 'public good', such as medical advancements.

Our review found that the issue of privacy online is itself not extensively researched, at least in comparison to other matters of public concern. As a relatively recent concept (the online aspect anyway), there is limited trend data available to track how public attitudes and actions on online data privacy have changed over the years. There are gaps in the evidence in terms of the views of different groups in society – including ethnic minority communities and disabled people. Meanwhile terminology is applied different across different studies; and much of the evidence is based on people's personal perceptions, rather than more objective measures. More and better evidence will be required in the future, to help inform our approach to these issues.

Interestingly, we also found that even though people are concerned about data privacy and don't necessarily act to protect this, most of us are quite confident in our ability to manage our privacy online.

The challenge now is to identify the steps we need to take as a society to ensure that this confidence is not misplaced and enable everyone to have the information and skills they need to make the right decisions for them about what data they share and how it is used.

Standing on a stage in San Francisco in early 2010, Facebook founder Mark Zuckerberg, responding in part to the site's recent decision to change the privacy settings of its 350 million users, said that as Internet users had become more comfortable sharing more information online with more people privacy was no longer a social norm (Johnson & Vegas, 2010). Because information about the users of social media was being sold by Facebook to advertisers and other third parties for targeted advertisements at higher

prices, Zuckerberg has a commercial interest in relaxing norms surrounding online privacy, but his attitude has been widely echoed in popular media.

The idea of a privacy paradox is commonly referenced in relation to SNSs; the idea that young people are sharing their private lives online, providing huge amounts of data for commercial and government entities, that older generations have fought and are fighting to keep private, because they do not fully understand the public nature of the Internet and its implications (Barnes, 2006). Some have gone so far as to assert that this practice may be the biggest generational split since the early days of rock and roll (Nussbaum, 2007).

There has been relatively little systematic research into privacy attitudes or actions among different age groups, or, for that matter, into most of the other major variables, such as race and gender, that may relate to how people present their private lives in online settings. Some evidence points to growing concern among Internet users about online privacy and increased concern over the ability of users to manage their information privacy online, for instance utilizing the privacy settings on popular SNSs (Marwick et al., 2010). A 2013 Pew study found that 50 percent of Internet users were worried about the information available about them online, compared to 30 percent in 2009 (Rainie, Kiesler, Kang, & Madden, 2013). Following the revelations that the U.S. National Security Administration was collecting the telephone and Internet metadata of its citizens, a Washington Post-ABC poll found that 40 percent of U.S. respondents said that it was more important to protect citizens' privacy even if it limited the ability of the government to investigate terrorist threats (Cohen & Balz, 2013). So privacy concerns may be increasing at the same time as conventional wisdom holds onto the view that younger people are less likely to act to control the privacy of their personal information in the online setting.

Privacy concerns an individual's ability to control what personal information is disclosed, to whom, when and under what circumstances. The unauthorized disclosure of personal information is normally considered a breach of privacy, although authorization and what is personal information are matters of dispute, particularly in an online context. Altman (1975, 18) describes privacy succinctly as "selective control of access to the self"

although this might go beyond legal definitions and hark back to related definitions of privacy focused on the right to be left alone, as framed by Warren and Brandeis (1890).

Many agree that disclosure and privacy are closely connected to fundamental characteristics of social life (Nissenbaum, 2011; Rule, 2009). Social life is powerfully structured by the context in which it takes place. People become acquainted based on many shared characteristics: some people you know from a local neighborhood—either current or past neighborhoods; others from sports clubs, church groups, hobby clubs, pubs or other leisure activities. Others are from current or prior education: school friends, university friends. Still others are based on common occupations or professions, or are people who work for the same company or organization. Almost everyone has family and relatives.

A variety of sociological theories suggest that privacy is part of the structure of social life. Rainie and Wellman, for example, describe how people who once experienced social life in relation to small and tight-knit communities are now becoming increasingly networked individuals with access to much larger and more loosely defined social connections (2012). With larger networks of looser ties, the practice of personal information sharing on a daily basis could become more challenging. Does information flow through the entirety of an individual's network or is it limited in some way?

Others focus more pointedly on specific realms where privacy expectations and values may be different. Nissenbaum describes the notion of 'context' in terms of roles, activities, norms, and values (2009, p. 133). She explains that a variety of factors represent, in an abstract sense, the social structures experienced in daily life. For example, Bourdieu's 'field theory' describes social systems wherein agents (individuals) are bounded by rules (norms) in specific fields (circumstances) (Martin, 2003). Nissenbaum argues that the different characteristics of different fields are crucial for considering what is and what is not a violation of privacy (2009).

Similarly Walzer describes a theory of justice in which context is crucial for deciding between right and wrong (1984) and Searle (and many others) explain how integral different social settings are to understanding social reality (1995).

Goffman explains the social psychology of these issues by describing how people act differently depending on who they are performing to. Individuals engage in "impression management" by presenting different versions of themselves to different audiences. The expectations and norms of the audience govern what personal information is presented and what is kept hidden (1959). Marwick and boyd extend this argument SNSs by looking at the "imagined audiences" of SNS users (2011).

The issue of audiences highlights a fundamental problem with privacy in some SNSs: Marwick and boyd (2011) describe 'context collapse', in which audiences that are separate offline collapse into a single unified online context. The management of this issue varies across social networking sites. 1 For example, Facebook started as a website restricted exclusively to university students at select elite US universities where it was bounded by the common norms of a small, self-selected population which was relatively homogeneous in terms of age, behavior and education. It has since diffused to become a transnational network with more than 1.15 billion active monthly users of all ages (Constine, 2013) where extreme heterogeneity is typical. SNS users often have difficulty conceptualizing the audiences that read their online posts and use the same account to address different audiences at different times (Marwick & boyd, 2011).

Heterogeneous contexts logically might lead to privacy problems: There are serious consequences when actions that are normatively appropriate in one context are revealed to members of another audience where norms are different; for example, a 24-year-old US high school teacher was forced to resign after a parent complained about a photo of her holding a glass of wine and a mug of beer while on holiday in Europe that was posted to her Facebook profile (Downey, 2011). Although the problem is particularly evident on Facebook, it appears on other SNSs as well. Twitter is primarily public and that can have serious consequences; for instance, Justine Sacco, a corporate communication specialist, was fired by her employer for what some saw as an insensitive tweet about AIDS in South Africa (Bercovici, 2013; Southall, 2013). Other examples abound. Even on Google+ there is nothing to prevent a naïve user from following the Facebook default that puts all their contacts into a single group.

This suggests that SNSs are a particularly good research site to investigate how people handle privacy. They create privacy problems that may make users more self-consciously concerned about privacy than in many other online situations.

There is a large body of literature that concerns online privacy; however, the number of published papers that use systematically collected data is very small. We were able to find only three peer-reviewed papers that addressed questions of privacy using a sample that could be generalized to a population: Taddicken (2013), who used an Internet panel to create a sample of 2,739 German adults, Turow and Hennessy (2007), who conducted a telephone survey of 1,200 US adults, and Milne and Culnan (2004), who constructed a sample of 2,468 US adults based on the Harris Poll Online panel. In addition, there are two Pew reports (Madden & Smith 2010; Raine et al., 2013), which use random digit dialing to construct a representative sample of US adults, and a research report by Hoofnagle, King, Li, and Turow that used a similar methodology (2010).

However, the majority of research in relation to privacy on SNSs uses convenience samples, often of university students. Early research in this area was conducted during the period that Facebook was limited to a relatively homogeneous population of university students, concluding that "only a vanishingly small number of users change the (permissive) default privacy preferences" (Gross & Acquisti, 2005). 2 However the rapid increase in the heterogeneity of SNS users and high levels of media coverage of privacy-related issues may have persuaded Internet users to become more concerned controlling their online privacy. A more recent study using a convenience sample of 200 Facebook users recruited via Amazon Mechanical Turk found that only 36 percent of content was shared using the default privacy settings (Y. Liu, Gummadi, Krishnamurthy, & Mislove, 2011).

Data Privacy India

Data privacy and protection is a fundamental foundation for an emerging data-driven economy like India. Permission marketing will be the next battleground brands or marketers will have to take cognizance of, as India transforms from a data-poor economy

to a data-rich economy. Permission marketing, a word coined by marketing expert Seth Godin in a book by the same name, is a non-traditional marketing technique that advertises goods and services when advance consent is given.

Let's look at some trends on how the Indian economy is moving towards being more and more data driven. At the last count, India has claimed first place across the world with 270 million Facebook users followed by the US which has 240 million Facebook users. Indians are leaving behind so much private data and information on this social media platform which is accessible to the world. The number of mobile wallet users in India is already over 250 million with Paytm having more than 100 million users and growing at a rapid pace. India, not China, is the world's fastest growing mobile payment market. The number of mobile wallet transactions is expected to surge to Rs 1 trillion in 2018. By 2025, digital transactions are expected to reach $1 trillion with four out of five transactions done digitally. There is little wonder then that the Reserve Bank of India (RBI), the country's central bank, has promulgated Know Your Customer (KYC) norms for wallet companies. The amount of privacy data that is being left behind with wallet companies is also enormous.

The number of mobile phone users in India is inching over 750 million consumers with smartphone users expected to reach 490 million by 2022. This will lead to a lot of mobile data usage and, therefore, personal data and information becoming available in the public domain. India's demographic dividend is also driving this change as it is estimated that India has about 390 million millennials and about 440 million generation Z, the generation that follows millennials. The Gen Z generation processes information faster and uses a lot of mobile applications like Snapchat, Vine and so on, apart from the usual popular social media apps. Therefore, the amount of personal data that will be at play – personal, behavioural, attitudinal and financial – so data privacy will be of paramount importance to protect the i-generation and citizens.

Poor data protection culture in India

In the past, very little attention has been paid in India to personal data and privacy. It's not uncommon for consumers here to share their personal information with different companies and entities – PAN card, Aadhaar card, mobile number, email id, address, and phone numbers – are easily doled out. Personal data is constantly misused by different companies or service providers. Data theft or selling data is very common but it needs to stop. When a data breach happens, the business, entity or individual responsible for the breach should be penalized.

Today, businesses pay very little heed to the privacy of the Indian consumer. If caught constantly calling or using customers' personal data to solicit business without their permission or consent, they should also be pulled up and penalized.

Data confidentiality and privacy is a primary right. Indian customers need to learn to exercise this right as the economy becomes digitally driven.

CHAPTER III

RESEARCH METHODOLOGY

INTRODUCTION

Research methodology involves specific techniques that are adopted in research process to collect, assemble and evaluate data. It defines those tools that are used to gather relevant information in a specific research study. Surveys, questionnaires and interviews are the common tools of research. Research methodology is adopted to check a certain theory and its application along a specific set of academic standards. This is mandatory so that all research methodologies perform a lot of functions. It applies to a number of jobs being done in research process.

Research methodology identifies the research activity in a true sense. It further specifies and defines the actual concepts. It further declares what sort of methods will be required for further inquiry. Moreover, how progress can be measured. Research methodology offers a platform to demonstrate how we can communicate research activity in true senses the field specific standards.

OBJECTIVES

General Objective

To understand the factors affecting privacy paradox and privacy protection behaviour.

Specific Objectives

- To understand the common characteristics the online social networkers share.
- To understand the motivating factors guiding people to use Internet.
- To understand their awareness on privacy issues in social networking websites.
- To understand the various methods they use to protect their privacy.

VARIABLES

- The level of user's online literacy
- The level of knowledge of privacy-enhancing tools
- The level of privacy and anonymity threat awareness

CONCEPTUALIZATION

The conceptual frame work has been derived from the conceptual understanding that has been developed from the literature review

DEFINITION OF CONCEPTS

1. THEORETICAL DEFINITION

a. Privacy Paradox - The privacy paradox is a phenomenon in which online users state that they are concerned about their privacy but behave as if they were not.

b. Social Networking Sites (SNSs) - A social networking site is an online platform that allows users to create a public profile and interact with other users on the website.

c. Youth - The period between childhood and adult age.

2. OPERATIONAL DEFINITION

a. Privacy Paradox – The privacy paradox studied on the difference of privacy awareness and behavior on the Internet and Social Networking Sites.

b. Social Networking Sites (SNSs) – Popular SNSs in India - Facebook, WhatsApp, Instagram, YouTube, Twitter, TikTok

c. Youth – Age between 18 and 30.

RESEARCH DESIGN

The research design refers to the overall strategy that is chosen to integrate the different components of the study in a coherent and logical way, thereby, ensuring that the research problem will be addressed effectively. It constitutes the blueprint for the collection, measurement, and analysis of data.

The researcher approached the study **quantitatively.**

- ***Quantitative Research*** is used to quantify the problem by way of generating numerical data or data that can be transformed into usable statistics. It is used to quantify attitudes, opinions, behaviours, and other defined variables – and generalize results from a larger sample population.

SURVEY DESIGN

Surveys are useful in describing the characteristics of the population under study. The researcher selected a sample of respondents from a population and administered a standardized questionnaire to them. The questionnaire was send through Google forms.

PILOT STUDY

A pilot study is a small scale preliminary study conducted in order to evaluate feasibility, time, cost, adverse events, and affect size in an attempt to predict an appropriate sample size and improve upon the study design prior to performance of a full-scale research project. The researcher conducted the pilot study among 5 respondents. From this the researcher understood the feasibility of the study. Appropriate modifications were made to enhance the instrumentality of data collection tools.

UNIVERSE AND UNIT OF THE STUDY

Universe

Youth of Thiruvananthapuram district.

Unit

Youth aged between 18 & 30 in Thiruavananthapuram who uses Social Media.

SOURCES OF DATA

1. Primary data: Primary data was collected through Google Forms.
2. Secondary data: Secondary data comprises of information from Documents, books, reports of surveys and studies, literature pertaining to the flood and it's after effects and other relevant publication.

TOOLS AND DATA COLLECTION

The researcher collected the data through Google Forms using a structured questionnaire.

QUESTIONNAIRE

The researcher selected a sample of respondents from a population and administered a standardized questionnaire to them. The questionnaire is a written document and that is completed by the researcher

SAMPLING

In sociology and statistics research, snowball sampling (or chain sampling, chain-referral sampling, referral sampling) is a nonprobability sampling technique where existing study subjects recruit future subjects from among their acquaintances. Thus the sample group is said to grow like a rolling snowball. As the sample builds up, enough data are gathered to be useful for research. When virtual social networks are used, then this technique is called virtual snowball sampling.

A sampling size of 72 is selected by the researcher through the sampling frame. Respondents selected where between the age of 18 and 30.

PRETEST

Before data collection the researcher tested the questionnaire in order to identify any problems such as unclear wording or the questionnaire taking too long to administer.

CHAPTER IV

ANALYSIS AND INTERPRETATION OF DATA

INRODUCTION

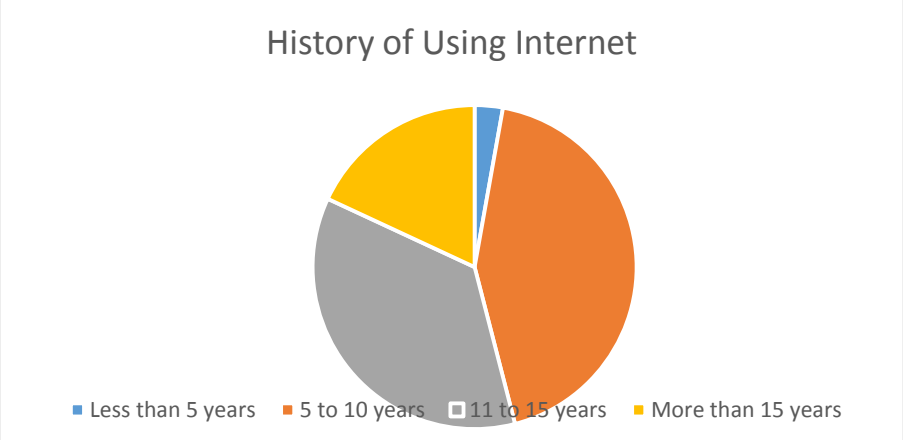
Quantitative data analysis is the process in which we move from the raw data that have been collected as part of the research study and use it to provide explanations, understanding and interpretation of the phenomena, people and situation which we are studying.

Table 1: Gender distribution of the respondents.

Gender	Frequency
Male	35
Female	37
Total	72

Table 1 shows the frequency distribution of the respondents. As you can see the respondents are almost similar in gender distribution.

Pie Chart 2: History of Using Internet

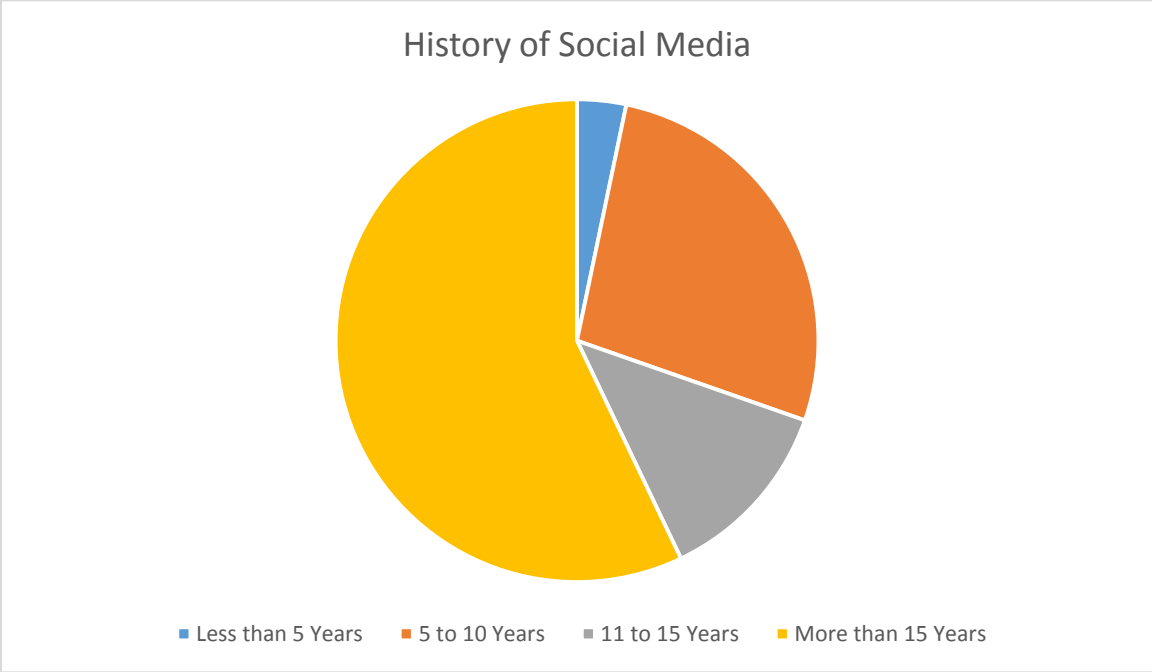


Pie Chart 2 shows the history of using Internet. The following was the data:

- Less than 5 years – 2.8%
- 5 to 10 years – 43%
- 11 to 15 years – 36.1%
- More than 15 years – 18%

Only 2.8 % of the population have used it for less than 5 years. Rest of the respondents have good experience in using Internet. Even 18% using it more than 15 years.

Pie Chart 3: Internet of Using Social Media

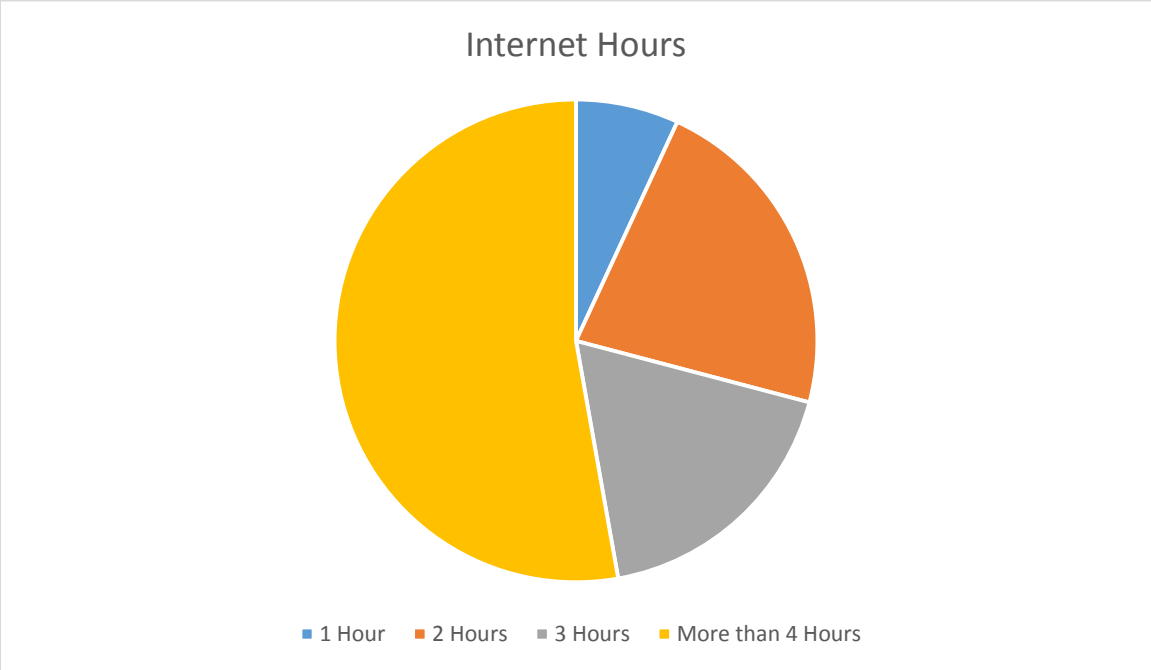


Pie Chart 3 shows the history of using Social Media.. The following was the data:

- Less than 5 years – 6.9%
- 5 to 10 years – 56.9%
- 11 to 15 years – 26.4%
- More than 15 years – 9.8%

Only 6.9 % of the population have used it for less than 5 years. Rest of the respondents have good experience in using Social Media. Even 83.3% using it from 5 to 15 years.

Pie Chart 4: Internet Hours



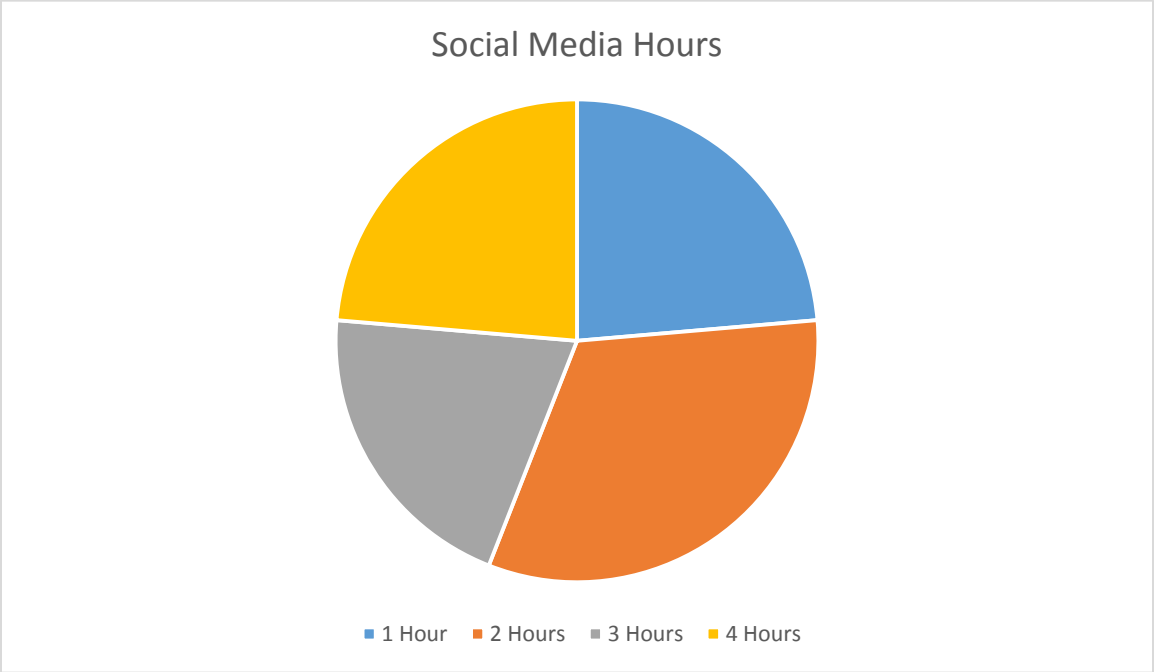
Pie Chart 4 shows how many hours per day, respondents connected to the Internet.

The following was the data:

- 1 hour – 6.9%
- 2 hours – 22.2%
- 3 hours – 18.1%
- 4 hours – 52.8%

The data shows that the respondents used Internet on an extensive basis. The hours specified here are the hours that the respondents were actually active on the Internet. But there are indications that nowadays people are never disconnected from the Internet. They usually always stay connected, either through mobile data or Wi-Fi. So the actual real- time Internet connection time is well more than the hours specified here.

Pie Chart 5: Social Media Hours



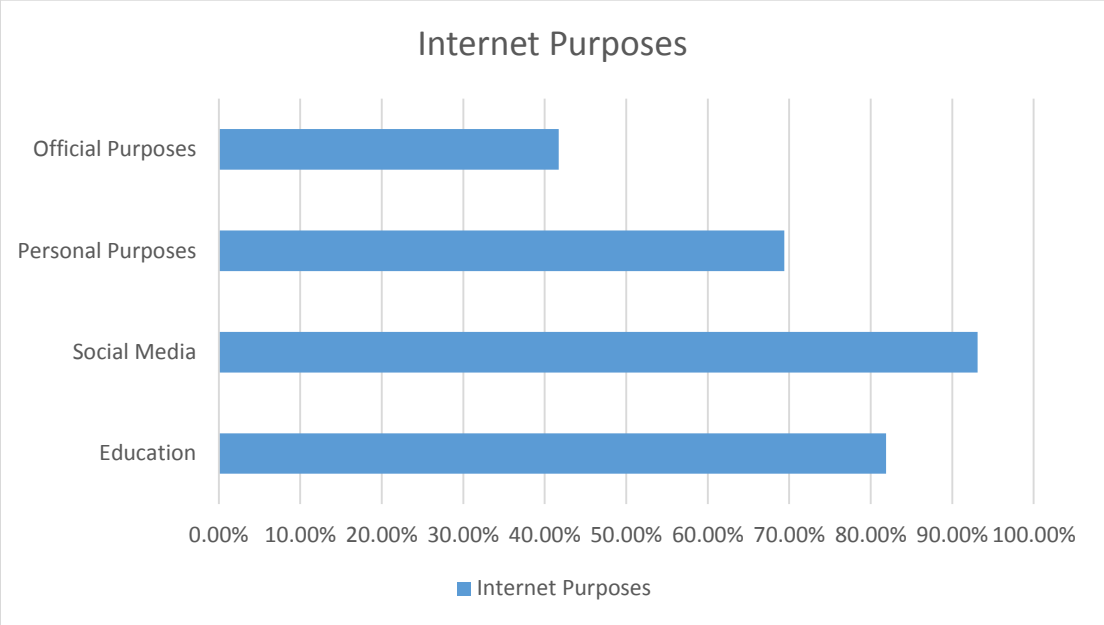
Pie Chart 5 shows how many hours per day, respondents connected to the Social Media.

The following was the data:

- 1 hour – 15.3%
- 2 – 36.1%
- 3 – 22.2%
- 4 – 26.4%

The data shows that the respondents used Social Media on an extensive basis. The hours specified here are the hours that the respondents were actually active on Social Media. But there are indications that nowadays people are never disconnected from Social Media. They usually always stay connected, either through mobile data or Wi-Fi. So the actual real- time Social Media time is well more than the hours specified here.

Bar Graph 6: Internet Purposes

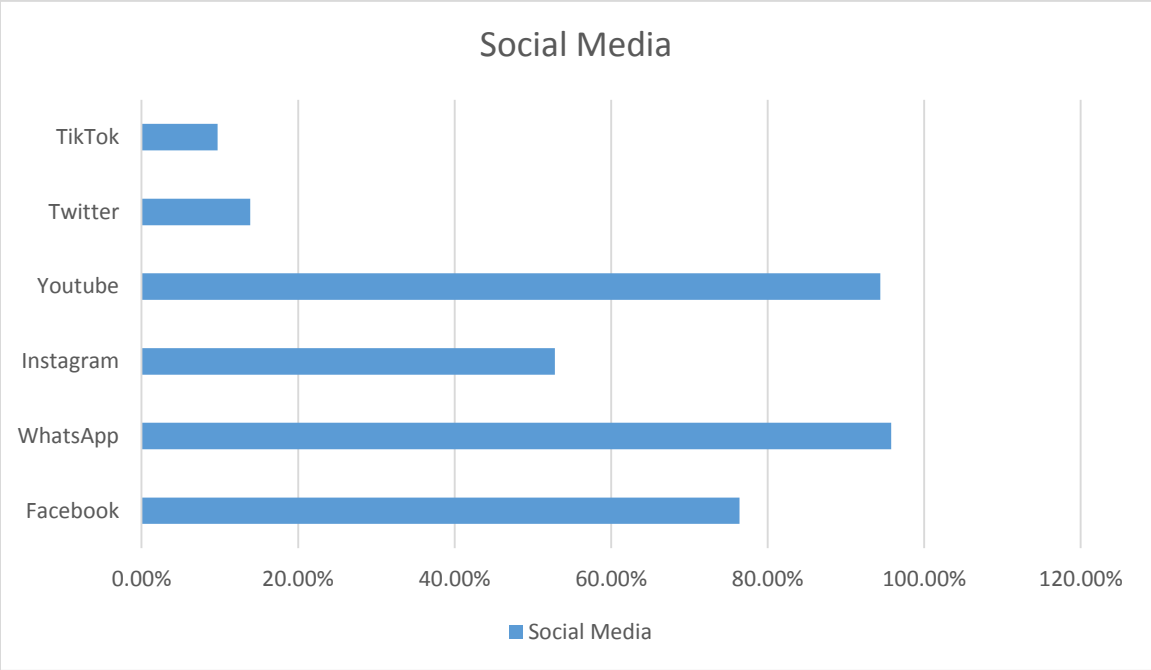


Bar Graph 6 shows the Purposes for the respondents used the Internet. The following are the data:

- Education – 81.9%
- Social Media – 93.1%
- Personal Purposes - 69.4%
- Official Purposes – 41.7%

Even though there are all other purposes for using Internet, almost all the respondents used Internet specifically for Social Media. Data leakage and Privacy loss can happen in almost all the above scenarios, but since almost everyone uses Social Media, the data loss can be severe.

Bar Graph 7: Social Media

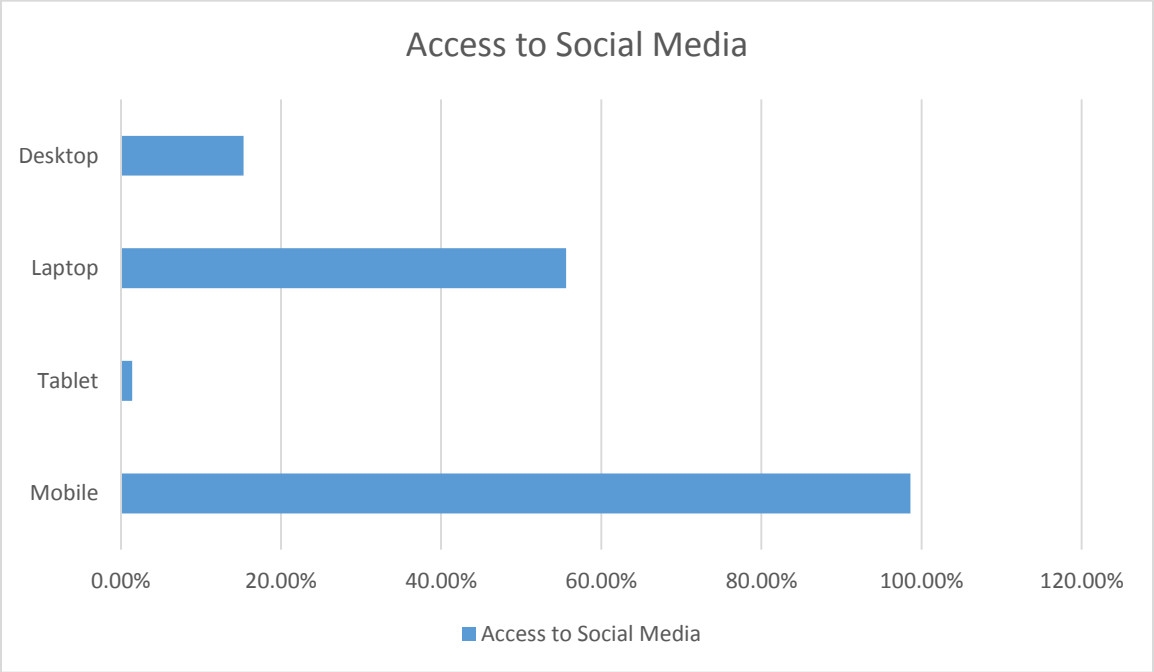


Bar Graph 7 shows all the Social Media Websites the respondents used. The following are the data:

- Facebook – 76.4%
- WhatsApp - 95.8%
- Instagram - 52.8%
- YouTube - 94.4%
- Twitter - 13.9%
- TikTok - 9.7%

Almost all the Social Networking Sites the respondents used were of big Social Media conglomerates. 94.4% respondents said that they used YouTube. YouTube owned Google has state of the art data analytical engines which recommends videos based on your watching history. This also shows how much data they track from the users. Almost all the respondents used at least one of the Social Media used by Facebook, a company notorious for its mishandling of user data.

Bar Graph 8: Access to Social Media



Bar Graph 8 shows how many devices the respondents used to get access to social media. The following are the data:

- Mobile – 98.6%
- Tablet – 1.4%
- Laptop – 55.6%
- Desktop – 15.3%

The data shows that the respondents used more than one device to get access to Social Media. That means if they're not on one device, they'll be on another. There have been reports on Social Media users that, once they get bored on one device they'll use it on another, extending the time spent on Social Media.

Table 9: I.T. Background

I.T. Background	Frequency
Yes	69.5%
No	30.6%
Total	100%

Table 9 shows I.T. background of the respondents. The respondents were asked if they had either an academic or an occupational background on the fields of Computer or Information Technology (IT). 69.5% of the respondents sure that they had an I.T. background.

Table 10: Computer Proficiency

Computer Proficiency	Percentage
Proficient	97.2 %
Not Proficient	2.8%
Total	100%

Table 10 shows Computer Proficiency of the respondents. The respondents were asked if they were proficient in Computer or Internet. 97.2% were sure that they were proficient.

Table 11: Internet privacy issues Awareness

Internet privacy issues Awareness	Percentage
Aware	84.7%
Not aware	15.3%
Total	100%

Table 11 shows the Internet privacy issues Awareness of the respondents. 84.7% of the respondents said that they were aware of the Privacy issues.

Table 12: Facebook–Cambridge Analytica data scandal Awareness

Facebook–Cambridge Analytica data scandal Awareness	Percentage
Aware	38.9%
Not aware	61.1%
Total	100%

Table 12 shows Facebook–Cambridge Analytica data scandal Awareness. Only 38.9% respondents said that they were aware. The Facebook–Cambridge Analytica data scandal was a major political scandal in early 2018 when it was revealed that Cambridge Analytica had harvested the personal data of millions of peoples' Facebook profiles without their consent and used it for political advertising purposes. It has been described as a watershed moment in the public understanding of personal data and precipitated a massive fall in Facebook's stock price and calls for tighter regulation of tech companies' use of personal data. It is curious that the 84.7% of the respondents who were aware of the privacy issues went down to 38.9%.

Table 13: Concern about privacy in Daily Life

Concern about privacy in daily life	Percentage
Concerned	93.1%
Unconcerned	6.9%
Total	100%

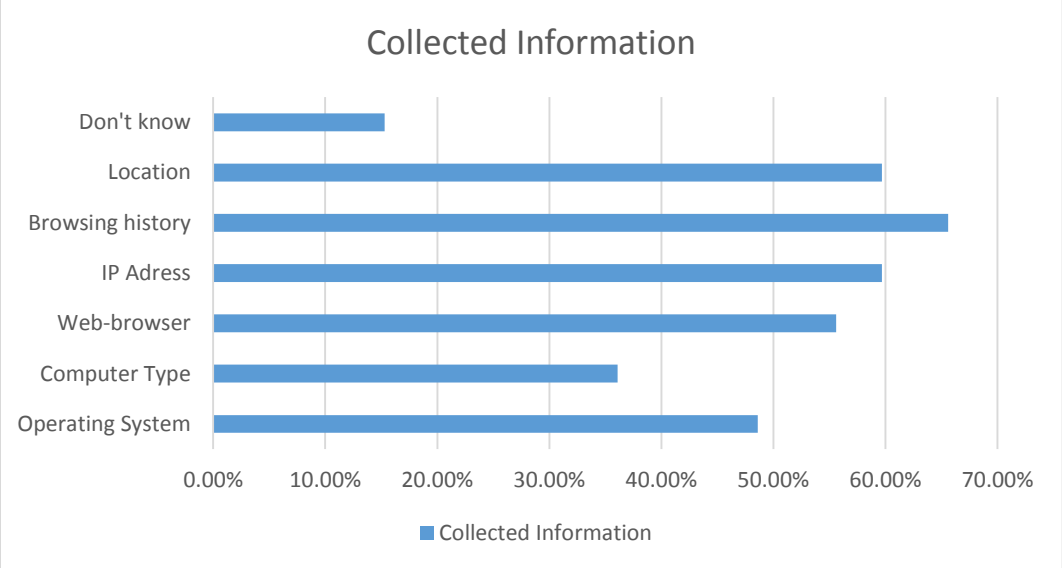
93.1% said that they were concerned about privacy in their daily life.

Table 14: Anonymity on the Internet

Anonymity on the Internet	Percentage
Felt anonymous	78.9%
Didn't feel anonymous	21.1%
Total	100%

78.9% felt anonymous. This feeling of anonymity while relaxing in their homes is one of the factors which fuel Privacy Paradox. When Internet began to be popular, people used Internet to escape from real life and be anonymous on the Internet. But when the data analytics engine became much more evolved, the fact is that while on the Internet, people are less anonymous than in their real life.

Bar Graph 15: Knowledge about the Information that is collected from users



The following were the outcome:

- Operating system. – 48.6%
- Computer type. – 36.1%
- Web-browser. – 55.6%
- IP address. – 59.7%
- Browsing history. – 65.6%
- Location – 59.7%
- I don't know – 15.3%

Table 16: Concern about Personal Information on Internet

Concern about Personal Information on Internet	Frequency
Concerned	95.8%
Unconcerned	4.2%
Total	100%

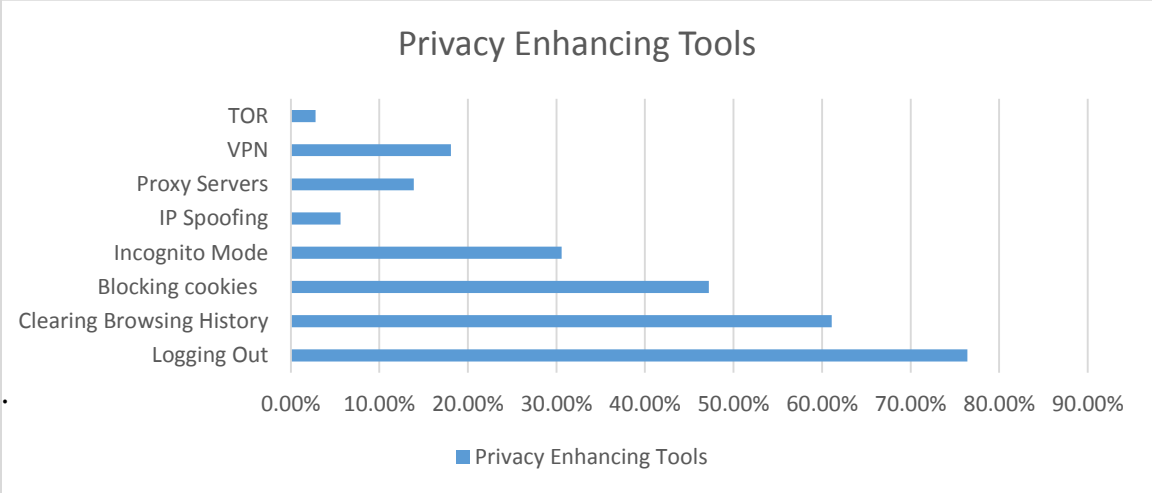
95.8% were concerned about the leak of personal information on Internet.

Table 17: Concern about Personal Information on SNSs

Concern about Personal Information on SNSs	Percentage
Concerned	94.4%
Unconcerned	5.6%
Total	100%

There was a slight dip in concern over personal information on SNSs.

Bar Graph 18: Privacy-enhancing Tools



The respondents were asked how many of the privacy-enhancing tools given below they used. The following is the data:

- Logging-out from online accounts – 76.4%
- Clearing history and other browsing details – 61.1%
- Blocking cookies – 47.2%
- Browsing via an Incognito Mode – 30.6%
- IP spoofing – 5.6%
- Using proxy servers. – 13.9%
- Using VPN (Virtual Private Networks) – 18.1%
- Using TOR – 2.8%

The privacy enhancement capability of the tools in the options given to them increased as they went down. The results expected was that usage of Privacy tools would decrease as it got more complicated. But there was a spike in the use of Proxy servers and VPN. This behaviour is partially due to the fact that Indian government recently banned access to a number of sites. VPN and Proxy servers gains people access to these websites.

Table 19: Use of complicated passwords

Use of complicated passwords	Percentage
Yes	29.2%
No	70.8%
Total	100%

Only 29.2% used complicated passwords.

Table 20: Use of save password option

Use of save password option	Percentage
Yes	45.8%
No	54.2%
Total	100%

There wasn't much variation in use of save password option by respondents.

Table 21: Often change password

Often change password	Percentage
Yes	23.6%
No	76.4%
Total	100%

Only 23.6% of the respondents often changed passwords. Changing passwords ensures protection of your data.

Table 22: Read Privacy policy

Read Privacy policy	Percentage
Yes	75%
No	25%
Total	100%

75% of the respondents read privacy policy. Reading Privacy policy could make you aware of the personal information an app or website could get from you.

Table 23: Download software from unfamiliar websites

Download software from unfamiliar websites	Percentage
Yes	84.5%
No	15.5%
Total	100%

84.5% downloaded from unfamiliar websites. Downloading from unfamiliar websites could result it data leakage.

Table 24: Use of simple password

Use of simple password	Percentage
Yes	22.6%
No	77.4%
Total	100%

77.4% of the respondents used complicated passwords ensuring protection of your data.

Table 25: Same password for different Online Accounts

Same password for different Online Accounts	Percentage
Yes	38.9%
No	61.1%
Total	100%

61.1% of the respondents used different passwords ensuring data protection.

CHAPTER V

FINDINGS AND CONCLUSION

Major Findings

The first objective - To understand the common characteristics the online social networkers share.

The youth has been using Social Media for more than 5 years and Internet for more than 10 years. They spend at least 4 hours daily on the Internet and Social Media. More than half of the respondents had an IT background and almost all of them were proficient in using computer and Internet. They were concerned about their privacy in daily life. The respondents were asked whether they felt anonymous while surfing the Web 78.9% felt anonymous.

The second objective to understand the motivating factors guiding people to use Internet. Almost all the respondents said that they used it to access Social Media, Education and Personal purposes. Almost all the respondents had more than one device to access Internet, making sure that they are always connected to the Internet.

The third objective was to understand their awareness on privacy issues in social networking websites.

More than 75% of the respondents were aware of the Internet privacy issues, but only a few of them were aware of the Facebook-Cambridge Analytica data scandal.

The fourth objective was to understand the various methods they use to protect their privacy.

They were aware of what all basic information that was collected from them. They used all the basic privacy enhancing tools to safeguard their privacy not using save password option, logging out from websites, clearing browsing history. But they didn't read privacy policies, they downloaded from unfamiliar websites, they didn't use complicated passwords and they never used the powerful tools to enhance their privacy.

The general objective was to understand the factors affecting privacy paradox and privacy protection behaviour.

Most people do care about privacy online; many of us fail to take the necessary steps to better protect our personal data. This may be because we don't know how to, choose not to, are not fully aware of the possible risks, or feel powerless to do so. The mismatch between attitude and action has been coined by researchers as the 'Privacy Paradox'.

There is no member fee for joining any of the Social Networking Sites. The price of access to the online world is not always free and the cost is not always obvious. As the 'old' saying goes – if the product is free, then you are the product. However the story isn't always quite as one-dimensional as headlines can often present it.

There are many hidden factors responsible for the Privacy Paradox to occur. The main and simple reason is comfort and exclusivety. Whenever the data of a user is collected and analysed, she/he will receive content based on her/his likes and dislikes. If the tools for data collection like browsing history, cookies, location and so on is cleared, then the user will stop receiving personalised content. News, friend suggestions, video recommendations and related products for online shopping all fall into the personalised content. Personal information is always collected. So whenever a user logs onto a website, the display screen of the Internet device is always filled with personalised and exclusive content. This makes a user welcome and comfortable the next time she/he uses the website.

Another factor is the feeling of anonymity and privacy. People always feel private within their boundaries of their home or their loved ones. Anonymity is when you are in a place surrounded by unfamiliar people. This feeling of anonymity while relaxing in the privacy of their homes is one of the factors which fuel Privacy Paradox. When Internet began to

be popular, people used Internet to escape from real life and be anonymous on the Internet. But when the data analytics engine became much more evolved, the fact is that while on the Internet, people are less anonymous than in their real life.

Conclusion

The youth claimed that they had good knowledge about Internet Privacy and Social Media. They even showed knowledge about how to safeguard themselves from data leakage and data theft. They knew simple steps like changing passwords, logging out from SNSs, and so on.

But when it came to complicated and uncomfortable tasks it seems that they stayed away not bother about such steps. For example TOR browser uses lots of encryption to safeguard user data. But this involves slowing down browsing speed and using a lot of power of the device. This abstains people from using it on a daily basis.

Privacy is a concept that has long been under study. But it has not gained much pace in India let alone Kerala. But Privacy Paradox exists in Kerala. Even though people might know how to protect their data they will prefer being comfortable than being safe.

Suggestions

- Make people more aware about how to protect their private information.
- Make people more aware of the importance of their private data.
- Make Internet and Social Media much more data friendly.
- Make better Privacy laws.
- Extensive studies could shed more light into the privacy paradox of India.

Bibliography

- 126 Amazing Social Media Statistics and Facts. (n.d.). Retrieved from https://www.brandwatch.com/blog/amazing-social-media-statistics-and-facts/
- Altman, I. (1975). The environment and social behavior: privacy, personal space, territory, crowding. Brooks/Cole Pub. Co
- Aristea M Zafeiropoulou, Kieron O'Hara, David E Millard, and Craig Webber. Location Data and Privacy: A Framework for Analysis. In Bernard Stiegler, editor, R´ eseaux sociaux : Culture politique et ing´ enierie des r´ eseaux sociaux, pages 185–200. FYP EDITIONS, 2012.
- Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. First Monday,11(9). Retrieved from http://firstmonday.org/ojs/index.php/fm/article/viewArticle/1394
- Bercovici, J. (2013, 23 Dec.). Justine Sacco And The Self-Inflicted Perils Of Twitter. Forbes. Retrieved January 8, 2014, from http://www.forbes.com/sites/jeffbercovici/2013/12/23/justine-sacco-and-the-self-inflicted-perils-of-twitter/
- Blank, G., & Dutton, W. H. (2012). Age and Trust in the Internet: The Centrality of Experience and Attitudes Toward Technology in Britain. Social Science Computer Review, 30(2), 135–151.doi:10.1177/0894439310396186
- Blank, G., & Reisdorf, B. C. (2012). The Participatory Web. Information, Communication & Society, 15(4), 537–554. doi:10.1080/1369118X.2012.665935
- boyd, d., & Hargittai, E. (2010). Facebook privacy settings: Who cares? First Monday, 15(8). Retrieved from http://journals.uic.edu/ojs/index.php/fm/article/view/3086
- Bullas, J. (2019, July 23). Is Social Media a Serious Threat to Your Privacy? - Infographic. Retrieved from https://www.jeffbullas.com/is-social-media-a-serious-threat-to-your-privacy-infographic/

- Carnegie UK Trust. (2018, September 28). How do we define, value and better protect our online privacy? Retrieved from https://medium.com/doteveryone/how-do-we-define-value-and-better-protect-our-online-privacy-70440ec16dfa
- Castells, M. (2014, September 8). The Impact of the Internet on Society: A Global Perspective. Retrieved from https://www.technologyreview.com/s/530566/the-impact-of-the-internet-on-society-a-global-perspective/
- Cohen, J., & Balz, D. (2013). Poll: Privacy concerns rise after NSA leaks. Washington Post. Retrieved December 16, 2013, from http://articles.washingtonpost.com/2013-07-23/politics/40862490_1_edward-snowden-nsa-programs-privacy
- Constine, J. (2013, July 24). Facebook's Q2: Monthly Users Up 21% YOY To 1.15B, Dailies Up 27% To 699M, Mobile Monthlies Up 51% To 819M. TechCrunch. Retrieved December 16, 2013, from http://techcrunch.com/2013/07/24/facebook-growth-2/
- Debatin, B., Lovejoy, J. P., Horn, A.-K., & Hughes, B. N. (2009). Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences. Journal of Computer-Mediated Communication, 15(1), 83–108. doi:10.1111/j.1083-6101.2009.01494.x
- Downey, M. (2011, October 10). Court rules against Ashley Payne in Facebook case. But more to come. Atlanta Journal Constitution: Get Schooled Blog. Retrieved from http://blogs.ajc.com/get-schooled-blog/2011/10/10/court-rules-against-ashley-payne-in-facebook-case/
- Dutton, W. H., & Meadow, R. G. (1987). A tolerance for surveillance: American public opinion concerning privacy and civil liberties. In K. B. Levitan (Ed.) Government infrastructures.,Connecticut: Greenwood Press.
- Dutton, W. H., & Shepherd, A. (2006). Trust in the Internet as an experience technology. Information, Communication & Society, 9(4), 433–451.

- Global social media research summary 2019. (2019, September 18). Retrieved from https://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/
- Goffman. (1959). The presentation of the self. Harmondsworth: Penguin.
- Gross, R., & Acquisti, A. (2005). Information revelation and privacy in online social networks. In Proceedings of the 2005 ACM workshop on Privacy in the electronic society (pp. 71–80).
- Hoofnagle, C. J., King, J., Li, S., & Turow, J. (2010). How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies? (SSRN Scholarly Paper No. ID 1589864). Rochester, NY: Social Science Research Network. Retrieved from http://papers.ssrn.com/abstract=1589864
- Indian Data Privacy Laws and EU GDPR. (n.d.). Retrieved from https://www.roedl.com/insights/india-eu-gdpr-data-privacy-law
- Internet users in India to reach 627 million in 2019: Report. (2019, March 6). Retrieved from https://economictimes.indiatimes.com/tech/internet/internet-users-in-india-to-reach-627-million-in-2019-report/articleshow/68288868.cms?from=mdr
- Johnson, B. (2017, February 21). Privacy no longer a social norm, says Facebook founder. Retrieved from https://www.theguardian.com/technology/2010/jan/11/facebook-privacy
- Levine, D. (1971). (Ed.) On Individuality and Social Forms. Chicago: University of Chicago Press.
- Lewis, K., Kaufman, J., & Christakis, N. (2008). The taste for privacy: An analysis of college student privacy settings in an online social network. Journal of Computer-Mediated

  Communication, 14(1), 79–100.

- Liu, C., Ang, R. P., & Lwin, M. O. (2013). Cognitive, personality, and social factors associated with adolescents' online personal information disclosure. Journal of Adolescence, 36(4), 629–638. doi:10.1016/j.adolescence.2013.03.016
- Liu, Y., Gummadi, K. P., Krishnamurthy, B., & Mislove, A. (2011). Analyzing Facebook privacy settings: User expectations vs. reality. In Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference (pp. 61–70). Retrieved from

  http://dl.acm.org/citation.cfm?id=2068823
- Livingstone, S. (2008). Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression. New Media & Society, 10(3), 393–411.
- Madden, M., & Smith, A. (2010). Reputation management and social media. PEW Research Center. Retrieved from http://ictlogy.net/bibciter/reports/projects.php?idp=1650
- Martin, J. (2003). What is Field Theory? American Journal of Sociology. 109(1): 1-49.
- Marwick, A. E., Murgia-Diaz, D., & Palfrey, J. G. (2010). Youth, Privacy and Reputation (Literature Review) (SSRN Scholarly Paper No. ID 1588163). Rochester, NY: Social Science Research Network. Retrieved from http://papers.ssrn.com/abstract=1588163
- Marwick, A. E., & Boyd, D. (2011). I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. New Media & Society, 13(1), 114–133. doi:10.1177/1461444810365313
- Madden, M., & Smith, A. (2010). Reputation management and social media. PEW Research Center. Retrieved from http://ictlogy.net/bibciter/reports/projects.php?idp=1650

- Milne, G. R., & Culnan, M. J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. Journal of Interactive Marketing, 18(3), 15–29.doi:10.1002/dir.20009
- Nissenbaum, H. (2011). A contextual approach to privacy online. Daedalus. 140(4): 32-48.Nussbaum, E. (2007). Say everything. New York Magazine, 12, 24–29.
- O'Neil, D. (2001). Analysis of Internet Users' Level of Online Privacy Concerns. Social Science Computer Review, 19(1), 17–31. doi:10.1177/089443930101900103
- Peluchette, J., & Karl, K. (2008). Social Networking Profiles: An Examination of Student Attitudes Regarding Use and Appropriateness of Content. CyberPsychology & Behavior, 11(1), 95–97. doi:10.1089/cpb.2007.9927
- PTI. (2019, July 23). Indian organisations lost ?12.8 crore to data breaches. Retrieved from https://www.thehindu.com/business/indian-organisations-lost-128-crore-to-data-breaches/article28681416.ece
- Rainie, L., Kiesler, S., Kang, R., & Madden, H. (2013). Anonymity, Privacy, and Security Online. Retrieved from http://www.pewinternet.org/~/media//Files/Reports/2013/PIP_AnonymityOnline_09051 Global Cyber Security Capacity Centre: Draft Working Paper Blank, Bolsover & Dubois The New Privacy Paradox page 333.pdf
- Rainie, L. & Wellman, B. (2012). Networked: the new social operating system. Cambridge, Mass.: MIT press.Rule, J. (2007). Privacy in peril. Oxford: Oxford UP.
- Searle, J. (1995). The construction of social reality. London: Allen Lane.
- Solove, D. J., 2007, "The future of reputation – gossip, rumor, and privacy on the internet", Yale University Press, New Haven & London.

- Sheehan, K. B. (2002). Toward a Typology of Internet Users and Online Privacy Concerns. The Information Society, 18(1), 21–32. doi:10.1080/01972240252818207
- Simplilearn. (2016, February 23). What Is the Major Impact of Social Media? Retrieved from https://www.simplilearn.com/real-impact-social-media-article
- Southhall, A. (2013, December 20). A Twitter message about AIDS, followed by a firing and an apology. The New York Times. Retrieved from: http://thelede.blogs.nytimes.com/2013/12/20/a-twitter-message-about-aids-africa-and-race/?_r=0
- Taddicken, M. (2013). The "Privacy Paradox" in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure1. Journal of Computer-Mediated Communication, n/a–n/a.doi:10.1111/jcc4.12052
- The privacy paradox is a privacy dilemma ? Internet Citizen [Web log post]. (2018, August 24). Retrieved from https://blog.mozilla.org/internetcitizen/2018/08/24/the-privacy-paradox-is-a-privacy-dilemma/
- Turow, J., & Hennessy, M. (2007). Internet privacy and institutional trust insights from a national survey. New Media & Society, 9(2), 300–318. doi:10.1177/1461444807072219
- Top five social media privacy concerns. (2018, January 24). Retrieved from https://www.reputationdefender.com/blog/privacy/top-five-social-media-privacy-concerns
- Walzer, M. (1983). Spheres of justice: a defense of pluralism and equality. New York: Basic Books.
- Warren, S. & Brandeis, L. (1980). Right to Privacy. Harvard Law Review. 4, 193.

Appendix

Questionnaire

1) What is your name?
2) What is your age?
3) What is your gender?
4) How many years have you been using Internet?
    a. Less than 5 years
    b. 5 to 10 years
    c. 11 to 15 years
    d. More than 15 years
5) How many hours per day, do you connect to the Internet?
    a. 1 hour
    b. 2 hours
    c. 3 hours
    d. 4 hours
6) What purposes do you use Internet?
    - Education
    - Social Media
    - Personal Purposes
    - Official Purposes
7) How long have you been using Social Media?
    a. Less than 5 years
    b. 5 to 10 years
    c. 11 to 15 years
    d. More than 15 years

8) How many hours per day, do you use Social Media?
    a. 1 hour
    b. 2 hours
    c. 3 hours
    d. 4 hours
9) What all Social Media Websites do you use?
    - Facebook
    - WhatsApp
    - Instagram
    - YouTube
    - Twitter
    - TikTok
10) How many devices do you use to get access to social media?
    - Mobile
    - Tablet
    - Laptop
    - Desktop
11) Do you have either an academic or an occupational background on the fields of Computer or Information Technology (IT)?
    a. Yes
    b. No
12) Are you proficient in computer/Interret?
    a. Yes
    b. No
13) Are you aware of the Internet privacy related issues?
    a. Yes
    b. No
14) Are you aware of the Facebook–Cambridge Analytica data scandal?
    a. Yes
    b. No

15) Are you concerned abouta range of information that others might learn about you in daily life?
    a. Yes
    b. No
16) Do you feel anonymous while surfing the Web?
    a. Yes
    b. No
17) Which of the following information do you think is collected, when you visit a website?
    - Your operating system.
    - Your computer type.
    - Your Web-browser
    - Your IP address.
    - Your browsing history.
    - Your location
    - I don't know
18) Are you concerned about the protection of your personal information on the Web?
    a. Yes
    b. No
19) Are you concerned about the protection of your personal information when using social network sites?
    a. Yes
    b. No
20) How many of the privacy-enhancing tools given below do you use?
    - Logging-out from online accounts
    - Clearing history and other browsing details
    - Blocking cookies
    - Browsing via an Incognito Mode
    - IP spoofing
    - Using proxy servers.
    - Using VPN (Virtual Private Networks)

- Using TOR

21) I use complicated passwords, even though it takes me more time, in order to reduce the risk posed on my personal information on the Internet.
    a. Yes
    b. No
22) I often change the passwords for my online accounts, even though it may be tedious.
    a. Yes
    b. No
23) I tend to read the "privacy policy" statement of a website asking me to submit personal details.
    a. Yes
    b. No
24) I tend to download software and content that I find to be important, even from unfamiliar websites despite the threat on my personal information.
    a. Yes
    b. No
25) When I am required to set a new password, I tend to use a simple one that is easy to remember.
    a. Yes
    b. No
26) I use the same password for different online accounts.
    a. Yes
    b. No