Online Privacy and Safety of Young Adults

Adrija Jana
Sahil Pradhan
Zayee Ajmera
Hari Harish
Darshan Shah

Written for

Internet Freedom Foundation

The authors are students of the Young Researchers for Social Impact (YRSI) Program conducted by Young Leaders for Active Citizenship (YLAC). YRSI identifies promising high schoolers and builds their capacity as critical thinkers and problem solvers to produce thought-provoking solutions to pressing issues that affect our societies today. This study was undertaken as part of the July 2022 edition of the program.

Disclaimer: The views expressed in this study are solely those of the authors and do not represent the views of YLAC as an organization.

Table Of Contents

1. Abstract **4**

2. Introduction **4**

3. Literature Review **5**

4. Methodology **6**

5. How Do Young Adults Navigate Social Media? **7**

5.1 Young Adults and Social Media 7

5.2 Young Adults and Privacy 7

6. Identifying Interactions and Threats **8**

6.1 Private Interactions 8

6.2 Interactions with Businesses 9

6.3 Interactions with Government Institutions 10

6.4 Interactions with EdTech 13

7. Analysing Social Media Platforms **14**

7.1 WhatsApp 14

7.2 Instagram 15

8. Introducing the Data Protection Bill **17**

9. Solutions and Our Recommendations **19**

9.1 Recommendations for the Government (Policy Recommendations) 19

9.2. Recommendations for IFF and Civil Society Organizations 21

9.3 Recommendations for Businesses and Social Media Platforms 23

10. Overall Limitations **24**

11. Conclusion **24**

12. Appendix 1: Survey **25**

13. Annexures **25**

14. Advocacy Material: Link to Open Access Design **25**

IMPORTANT DEFINITIONS

Young Adults: For the scope of our paper, individuals aged 13-24 are considered "Young Adults".

Social Media: Digital platforms for people to connect, create and share content, and get access to news, opportunities, and online services. For the scope of this paper, Social Media is limited to "WhatsApp" and "Instagram".

Privacy: The state of being alone or out of the sight and hearing of other people so that one can do things undisturbed.[1]

Personal data: Personal information like date of birth, gender, address, name, signature, mobile number, bank account details, and even trends on how a user spends their time on the internet are classified under it. These data points are sensitive and can compromise one's internet safety.

Information Privacy: Indicates that the person generating personal data is the owner of that data, and should play the most important role in regulating how that data is used.

User Profile: Data of customers being used by social media platforms, businesses etc. to create a profile (record of personal data + metadata) of them.

Threats: A potentially possible accident that may have an undesirable effect on the supported system and information resources

Attacks: Unauthorized access to a system and corresponding information resources

Online Safety: Protection of user's data and safeguarding it from misuse through policies, legal proceedings, and self-awareness.

Algorithm: A way of sorting posts in a user's feed based on relevancy instead of publish time. This is done by collecting user personal data and allowing for social media platforms to understand user behavior and preferences. Algorithms then showcase content based on user preferences.

Echo chambers: Bubbles on social media that keep reinforcing your own opinions to get you to agree with them more.

[1] Heng Xu, Information Privacy Research: An Interdisciplinary Review, ww.researchgate.net/profile/Heng-Xu-3/publication/220260183_Information_Privacy_Research_An_Interdisciplinary_Review/links/543157530cf29bbc12789742/Information-Privacy-Research-An-Interdisciplinary-Review.pdf

[2] Barnhart, Sprout Social, 2021, https://sproutsocial.com/insights/social-media-algorithms/

1. Abstract

The topic of privacy, a universally recognized basic human right, has assumed a completely new dimension in the recent past. The internet has increasingly become a staple for young adults across the globe. Complementing this rise in internet usage is the rise in technologies that can gather and process large amounts of data for both use and misuse. In this context, this research will explore issues around the privacy and safety of young adults online, with a special focus on social media platforms.

Through extensive literature review, various forms of young adults' online interactions and the potential threats ensuing from these interactions have been compiled and interpreted. In addition, a survey was conducted and relevant stakeholders were interviewed to understand awareness and perceptions of privacy and safety online. According to a survey by YOLO, WhatsApp and Instagram are the social media platforms used most by young adults[3]. Therefore, to understand the root of privacy issues, the privacy policies of these two platforms were studied in detail. Finally, the measures undertaken by the Indian government addressing these issues, namely the new Data Privacy Bill, were critiqued concerning its likely implications on the comprehensive safety and growth of young adults.

Based on our study, recommendations for governments, social media platforms, and also parents were made to improve the safety and privacy of young adults online.

2. Introduction

Young adults are undoubtedly the most active online today, leading the digital space to curate and consume content on world-wide social media platforms.[4]

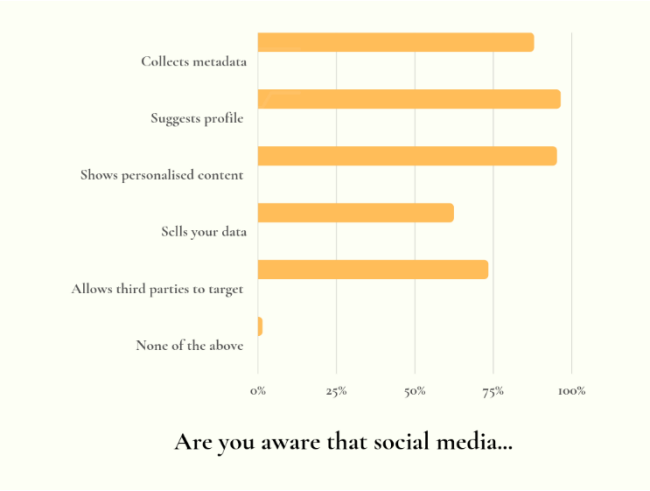


Figure 1: Awareness of Young Adults regarding social media policies (Primary Data)

In this digital era, social media platforms and other online services collect huge amounts of personal and behavioral data to create the "most optimal user experience", may it be for more appropriate advertisements or even suggestions for new shows to watch. This can also lead to a situation where bias and malpractice in the handling of data are incorporated into the algorithm and in turn, perpetuated. All of this generates concern for the online safety and privacy of young adults and their personal and data security on the internet.

The results of our survey showed that while **95%** of our target audience are aware of how social media uses user data to make recommendations, only **62%** are aware that companies sell this data for a higher revenue. Likewise, **82%** of young adults are aware about privacy and keep their Instagram accounts private. **58%** of young adult Instagram users restrict their followers and **61%** are apprehensive to share their tags with strangers.

[3] IGPP, SMM, YOLO Survey, 2020, https://drive.google.com/file/d/1Hh-jAvU1n-mPDopCp-YLod4qbIVmp9lV/view
[4] IGPP, SMM, YOLO Survey, 2020, https://drive.google.com/file/d/1Hh-jAvU1n-mPDopCp-YLod4qbIVmp9lV/view

India does not yet have a comprehensive law governing the data privacy of citizens. The provisions available in this regard are few, some vague, and scattered across case laws and other legislations.

The Information Technology (IT) Act was passed in 2000 to deal with cybercrime and electronic commerce in India but it doesn't address privacy issues and doesn't deal with nuances of cybersecurity[5]. In 2021, the IT Rules were introduced but it doesn't protect data of social media users from the government and thus makes the ruling party an arbiter to suppress speech as they feel right. The rules allow overboard grounds for restricting online content and require messaging services to violate "end to end encryption" when needed by the government. [6]

Important case law in this regard is the landmark Puttaswamy vs. Union of India case (2017)[3] which held that the Right to Privacy was a fundamental right of citizens and also laid down certain provisions regarding the privacy of children online but didn't provide enough tools to ensure how data privacy should be prioritized. However, even when we look at these three together, they are not adequately detailed to cover all aspects of digital privacy and the online safety of citizens.

In this context, in 2019, a new Personal Data Protection (PDP) Bill was proposed by the Parliament[7] which, among other provisions, proposes setting the age of digital consent to 18 and requiring parental consent for all data collection and processing for individuals under that age but the proposed bill too has its own set of flaws that we will discuss in the course of the study.

How do Young Adults use social media? How do they interact online and what threats do these interactions pose to their safety and digital privacy? How feasible is the new data privacy bill and will it operate in the interest of citizens? This paper aims to seek an answer to all these questions through primary and archival research.

3. Literature Review

For young adults who have access to a wide range of internet services and multiple social media platforms, data privacy is of utmost importance.

Personal data protection (PDP) is a major element for ensuring privacy of social media users. It comprises laws, policies, guidelines, and procedures through which access to personal data is limited even to the platform itself. This determines how the government, third parties, and the platform itself processes personal data while making sure to keep the public's privacy safe. It is known that the main reasons for breach in data privacy in personal data protection are of two forms: threats and attacks [8].

In many cases, websites play the role of an "open door" – during the preliminary registration or at the first visit with just one "click" users can accept the Privacy Policy without reading the policy itself. The result is full acceptance of all conditions without the user being consciously aware of what they agreed to.

In other cases, the user's data is stored after one visit only and automatically transferred to the social media platform's database without the owner's knowledge and consent. Indicative is the fact that only 54% of social network users think that they are informed about the conditions for collecting personal data and their next use

[5]MeITY, Govt of India, 2017, https://www.meity.gov.in/content/information-technology-act-2000-0
[6]PRS India, 2021, The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021
[7] Bharti and Iyer, 2022, Data protection Bill puts Indian children at a disadvantage. Here's how - The Economic Times
[8] Supreme Court Observer, 2017, (Puttuswamy vs. Union of India)

when they join a social networking site or register for an online service. [9]

In some cases, social media platforms may not provide information about the Privacy Policy or collect more personal information than they require.[10]

According to the data collected by YOLO, respondents across all age groups use the internet for learning, professional, socializing and recreational purposes. Amongst the 18–25 age bracket, Instagram is the widely used social media platform, while those above the age of 25 prefer to use Facebook. The study concluded that despite enabling personal, social, and professional networking, high internet usage is detrimental especially for the youth due to over-usage.[11]

Privacy, both as a basic human right and a rapidly evolving ethical aspect in the modern day, needs to be paid greater attention to, especially in the context of the increasing use of online facilities by young adults. *"I like to keep my information private. I am not comfortable with people having unlimited access to my private information because the digital atmosphere these days can be extremely exploitative."* said a respondent from our survey.

4. Methodology

Our research area is focused mainly on India, as the main objective is to navigate data privacy and threats to young adults online in India. Our research includes primary data collected via survey. The study authors disseminated the survey via various channels online, including social media platforms. Consent of survey participants was taken before using the data provided by them and anonymity was maintained. Participants were informed of the risks involved in taking the study. The survey was conducted with a pool of 91 people hailing from diverse backgrounds from India. Out of the respondents, 30 percent identified as male, 63 percent as female and 7 percent as non binary.

The analysis of the data collected has been visualized in the study using graphs and charts.

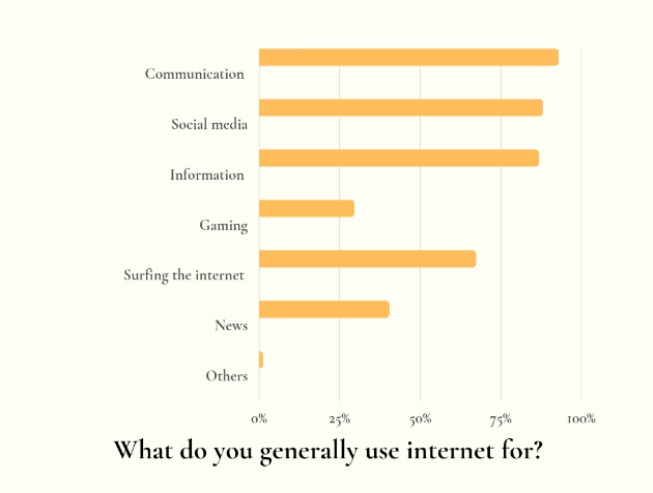


Figure 2: More than 75% of the young adults who took our survey said they use the internet for social media, which makes it the second most chosen option after "Communication." (Primary Data)

The secondary data used in the study has been collected from online archives, existing research studies, and policy and case study documents with proper acknowledgment and citations wherever necessary. For a deeper understanding of the topic at hand, some of the information used in the study has also been drawn from stakeholder interviews with lawyers, teachers, students, and youth organizations, again with proper acknowledgment wherever applicable.

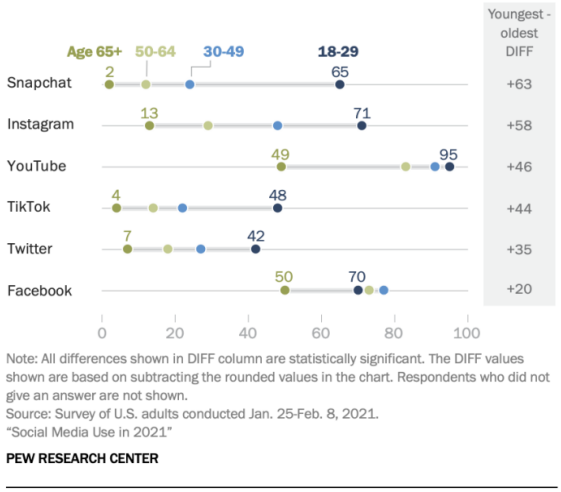
[9] Romansky, Research Gate, 2014, (PDF) SOCIAL MEDIA AND PERSONAL DATA PROTECTION
[10] Vasilis Stavropoulos, Frosso Motti, Mark D Griffiths, 2021 Risks and Opportunities for Youth in the Digital Era: A Cyber-Developmental Approach to Mental Health
[11] Bohra, 2020, Social Media Matters, Patterns of Internet usage among youth in India

5. How Do Young Adults Navigate Social Media?

5.1 Young Adults and Social Media

Research by PEW shows that Instagram is the most used social media platform with 76% of 15-21-year-olds being customary users.[12]

PEW Research also shows that young adults are more aware as compared to adults, especially regarding data privacy cookies and sharing personal information online. Young adults are also shown to follow self-censoring, further emphasizing that 15-21-year-olds are aware that information is hard to control once shared on the internet[13].



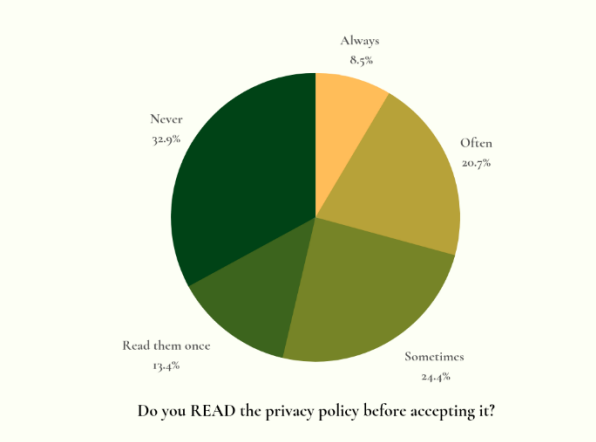


Figure 3: 32.9% Young Adults say that they never read the privacy policy on a social media platform before accepting it, which is alarming. (Primary Data)

According to the data collected by YOLO, most of the Indian youth comprising 85% of non–adult users have access to smartphones.[14] Most of them are online five hours a day and 80% admitted to using social media. A growing number of youths watch videos on OTT platforms other than YouTube. However, there's a lack of awareness about privacy and safety control measures on online platforms. Nearly 30% of respondents admitted to having shared sensitive information online while half of them accepted to have watched online pornography and 40 % agreed to know those who have watched pornographic content on the internet[15].

5.2 Young Adults and Privacy

Studies from Harvard, Berkeley, and UPenn show that while young adults are extremely adamant to keep their data private, they care more about an invasion of privacy from people they know, like parents, teachers, and family, rather than external companies[16].

Privacy is important to all young adults - however, it is multifaceted and has many different perspectives to look at. Privacy controls employed by these young adults to filter what their parents can see are avoided completely when parents request family members to oversee their children's accounts. Research shows that young adults believe that just because something is on the internet does not mean it is meant to be read by everyone, and it is

[12] PEW Research, Social Media Use in 2021, Social Media Use in 2021 | Pew Research Center
[13] PEW Research, Social Media Use in 2021, Social Media Use in 2021 | Pew Research Center
[14] Anurag Singh Bohra, Patterns of Internet Usage Among Youths In India, Patterns of Internet Usage Among Youths In India
[15] Anurag Singh Bohra, Patterns of Internet Usage Among Youths In India, Patterns of Internet Usage Among Youths In India.
[16] Jennifer Valentino-DeVries, Do Young People Care About Privacy Online?, Do Young People Care About Privacy Online? - WSJ

still an invasion of their privacy. They enjoy the comfort of sharing publicly via anonymous or other accounts. However, all data is uploaded with certain boundaries in mind, which when violated causes a breach of privacy[17].

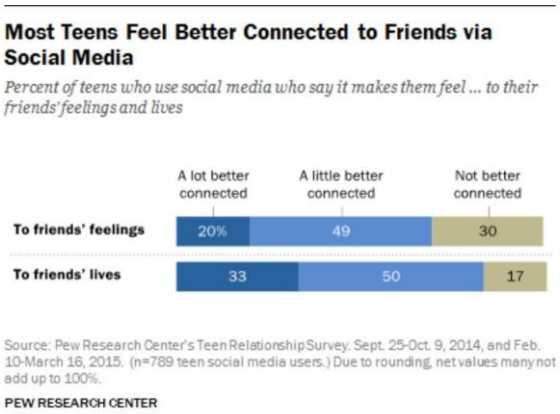
When asked about what young adults can do to stay safe online, a survey respondent said, *"Prevention is better than cure, so young adults should take the necessary preventive measures like regularly changing their passwords and not sharing it with anyone, double step verification, being extremely careful about online contacts, being aware of their data that websites and companies use. Also, they should be aware of the basic steps to take in case there is a violation of their data privacy."*

When asked about the role of schools in ensuring online safety of students, Dr. Cyrus Vakil, Principal of the Bombay International School, said, *"All school email accounts (assigned to students, teachers and parents) are password-protected and students are repeatedly told not to share passwords with anyone. In addition to Net citizenship and safety taught in ICT classes there have also been presentations made by external experts and parents in the field."*

6. Identifying Interactions and Threats

6.1 Private Interactions

The original motivation behind the innovation of social media was to enable individuals living physically very far away to connect. Research reveals that this is still one of the primary reasons why Young Adults use social media platforms- to stay connected and build new connections.



Social media plays a critical role in connecting young adults and allowing them to interact with people around the world. Nearly two-thirds (64%) of teens who have made a new friend online say they have met them on a social media platform. Two-thirds (62%) of teens say they've shared their social media username with a brand new friend as a way to stay in touch.[18]

Social media has started acting as a platform for community building, and many teens have reported that they received support from their online community during tough times.[19] As research from Teen and Tween showed[20], "Social media that's humorous or distracting or provides a meaningful connection to peers and a wide social network might even help teens avoid depression."

Apart from direct messaging, another way to connect with other individuals online is to interact with their posts via likes, shares and comments. These actions are also fast becoming a very common and much-preferred way of securing validation and support on social media platforms.

[17] Steeves, 2014, (https://www.researchgate.net/publication/289839760_Young_People_Online_and_the_Social_Value_of_Privacy)
[18] Lenhart, Pew Research Centre, 2015, Social Media and Teen Friendships | Pew Research Center
[19] Anderson & Jiang, Pew Research Centre, 2018, Teens, Social Media & Technology 2018 | Pew Research Center
[20] Robb, Common Sense Media, 2015 Tweens, Teens, and Screens: What Our New Research Uncovers | Common Sense Media

Potential Threats

While social media is one of the fastest and easiest ways to build and maintain interpersonal relationships, Young Adults often forget to take into consideration the various threats that might arise from these interactions to their safety and private information.

Young Adults often share private information with online friends without properly getting to know them first. For example, underage sharing of nudes has become a very common phenomenon online. This information might be used in malafide ways harmful to the victim, and it can be very difficult to find a way out of such situations.

For example, in early 2020, the shocking "Bois Locker Room" incident online came into focus. A group of South Delhi teens (mostly schoolboys) created an Instagram group chat called Bois Locker Room to share photos of women (many of them underage). The group involved discussions objectifying women and graphic sexual language[21]. The incident came to light when screenshots from the group chat were shared online. Moreover, a considerable number of Young Adults also say that other people often post things about them online that they are uncomfortable with and have not consented to.[22] This tells that there needs to be greater focus and attention on threats from personal interactions on social media.

6.2 Interactions with Businesses

In the modern era, business owners, in pursuit of making their businesses "tech savvy", to the great delight of everyone around the world, have ensured that all transactions of data and information happen online to ensure easy outreach and communication. For this reason, young adults' interactions with businesses primarily branch off the previously mentioned platforms of social media.

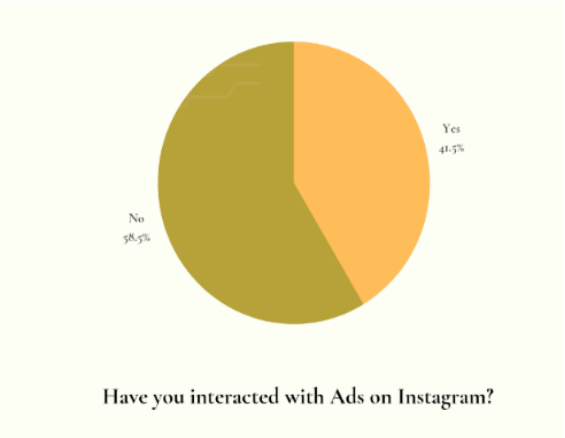


Figure 4: 41.5% of Young Adults on Instagram have interacted with Businesses via Ads (Primary Data)

Social media remains the key component of the omnichannel user experience. Businesses utilize them to their maximum potential to ensure maximum customer interest and retention. Customers interact with businesses in the following manners online – Discovery of the business, Research about the business, Engaging with the product, Signing up for and purchasing the product, and Promotion of the product. During these steps, there may be various reasons for a breach of privacy or unknown sharing of data we need to ensure we are aware of.

Potential Threats

Studies done in 2021 show that 72% of small businesses online have been victims to at least 1 cybersecurity attack in the past 12 months, showing us that we should take these threats very seriously.[23] Below are a few methods through which data could potentially get leaked.

[21] India Today, 2020, Bois Locker Room: 10 things you need to know about scandal that has rocked Indian social media
[22] Anderson & Jiang, Pew Research Center, 2018, Teens, Social Media & Technology 2018 | Pew Research Center
[23] Delvin, University of Cincinnati, 2021, Small- and medium-sized businesses are vulnerable to cybercrime | University Of Cincinnati

1. **Accidental Sharing**: While this may not be an unethical move by the company, Young Adults often do not understand that the information they provide will remain with the company permanently even after the interaction is completed. A shocking number of incidents have occurred where a company's own employees often leak this data without meaning to, by either accidental sharing, mishandling, or misplacement. In a Shein report in 2018, 40% of senior executives were said to attribute their most recent security incident to these behaviors.[24]
2. **Overworked Cybersecurity teams:** IT administration has a surprising percentage of employees who feel burnt out and more than 2/3rds have considered leaving this field due to the stressful environment. The general fatigue and loss of morale leave the company more exposed to threats.[25]
3. **Ransomware and Phishing:** Ransomware attacks are highly expensive digital cash grabs that prove highly dangerous and are targeted at local municipalities and midsize businesses. Phishing scams are baits targeted at customers to make them click on a stray link and induce a virus into their systems to have free access to data.
4. **Bad password hygiene:** Google studies conclude with results saying that 1.5% of all login credentials online are very vulnerable[26] to credential stuffing attacks and easy foreign access to data. Furthermore, if a data breach does occur and a login credential is exposed, if the same credentials are used across various platforms, they are all subject to data theft.

Apart from the leaking of data, privacy is still violated via acquiring information non-consensually for the sole purpose of targeted ads for customer cherry picking. Information is also acquired with the help of cookies. These cookies, which the users may accept, can tend to have unknown side effects including user profiling and development of echo chambers.

For this reason, young adults need to be aware and think practically to avoid these threats to privacy. Businesses should focus on establishing a certain level of trust and properly enlighten the user about the risk profile before proceeding with the interactions. They should set predefined limits to data collected and improve on customer privacy policies to ensure that only vital data is collected.

When asked about what businesses could do to improve data privacy of customers online, we found conflicting opinions from our respondents. One said, "They don't care. The bottom line is to increase profits. Sure, if consumers place more pressure they'll enact more privacy measures, but only because it hurts the bottom line." Another said, "They are doing pretty fine. I think we need to educate people that we can turn off personalized ads even though I feel they are helpful to a certain level." This shows that there is an urgent need for social media platforms and businesses to build trust level with their users, and this can only be done through more clarity.

6.3 Interactions with Government Institutions

Social media's role as a tool for engagement and activism is more widely known now. Between the government and the common folks, social media now acts as a medium of contact and the last decade has been a testimony to the growing power of social media on public opinion and awareness.

A decade ago, in December 2010, a series of protests popularly referred to as the "Arab Spring" changed the way people look at social media as a tool for change[27]. As protestors used social media and the internet to discuss

[24] Cyware, 2018, SHEIN data breach saw hackers steal 6.42 million users emails and encrypted passwords stolen | Cyware Alerts
[25] James, LinkedIn, 2017, Cybersecurity Professionals Wanted: Study Shows Teams Are Overworked, Undertrained
[26] Cyware, 2019, Google warns 1.5% of all passwords used across the web are vulnerable to credential stuffing attacks | Cyware Alerts - Hacker News
[27] PEW Research Centre, 2012, The Role of Social Media in the Arab Uprisings | Pew Research Center

uprisings and protests, organize and mobilize both pro and anti-government protests, the movement paved the way for future revolutions and the role of social media in them. In recent memory, movements like #BlackLivesMatter[28] and #MeToo[29] have cemented the role of social media as a platform to raise voices against discrimination and injustice.

Not surprisingly, politicians and senior government officials in India have been taking cues from around the world and are using social media platforms to shape the dialogue with citizens. Most, if not all, leaders, representatives, and politicians, as well as government bodies, maintain operational accounts on social media platforms, especially Twitter. According to the Government of India, social media users in the country have surpassed the 500 million mark. Signifying the volume of politically motivated content, a 2019 CSDS-Lokniti, and Konrad Adenauer Stiftung survey determined that one in every three Indian citizens on social media consumes political content daily or regularly.[30]

To young adults, reassurance during chaotic episodes is an important component of wellbeing. A more targeted use of the internet in reaching young adults is for promoting and conducting government-held programs and policies.

Potential Threats

A government with its own benefits in mind could cause havoc on data privacy breaches using social media platforms to stay incumbent. A breach of privacy in this sense can mean the use of personal data trends on how young adults interact with social media to influence opinions, forceful extraction of mass public personal data using loopholes in laws, and threatening legal action on social media platforms if they fail to comply.

In early 2021, the Indian Computer Emergency Response Team (CERT-In) passed guidelines that mandated companies offering virtual private network (VPN) services in the country to record and store the details of their users. This has resulted in ExpressVPN removing its servers from the country and more companies are expected to follow in its footsteps.[31]

The Ministry for Electronics and Information Technology (MeitY) has released proposed amendments to Part I and II of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, also known as IT Rules. The proposals mandate social media platforms to establish a grievance redressal mechanism that will allow users to request for the removal of content or a user or complain against the removal of content or blocking of any user on their platform through grievance officers and then the Grievance Appellate Committee that will include a chairperson and other members appointed by the government. The 2021 IT Rules makes it harder for social media platforms to adhere to the guidelines of the law without violating their own user privacy policy. Governmental indirect control over personal data is a loophole in the laws. Using the current IT laws 2021 and the proposed PDP Bill, the government can forcefully infringe on social media platforms and have access to the personal data of the public.

The Disha Ravi vs State of India case[32] is an example of how the government can violate the Right to Privacy that came about by the Puttaswamy vs Union of India 2017. This judgment clearly settled the position of law and

[28] Olson, 2021, Roles of Social Media in the Black Lives Matter Movement During COVID-19
[29] Ziles, 2018, The #MeToo Movement Shows The Power Of Social Media
[30] Jose, 2021, The Politicization of Social Media in India – South Asian Voices
[31] Business Insider, 2022, Indian government's VPN guidelines will impact over 270 million users as VPN providers have no option but to leave the country | Business Insider India
[32] Columbia, 2021, The Case of Disha A. Ravi - Global Freedom of Expression

clarified that the Right to Privacy could be infringed only when there was a compelling state interest for doing that. In Ravi's case, the Court made pertinent observations on the applicability of the law of sedition which was used to violate her privacy. In so doing the Court upheld a citizen's right to dissent and protest, which rights are protected under the fundamental right to free speech – it further stated that dissent and divergence of opinion were a sign of a healthy democracy.

In July 2022, Twitter asked the Karnataka High court to overturn some government orders to remove content from their platform, in a legal challenge that alleges abuse of power by officials. Twitter also argued in its filing that some of the orders failed to give notice to authors of the content and that some were related to political content posted by official handles of political parties.[33] This is not only a violation of the Right to Privacy protected under Article 21 of the Indian constitution but also can be a violation of the Right to Freedom of Speech and Expression protected under Article 19(1)(a) of the Indian constitution.

Government bodies can also manipulate public opinion and misuse personal data trends, such as what kind of content you look up on the internet or how much time you spend on which Meta platform, for gaining favorable election outcomes or larger public acceptance of botched policies.

Around the time of the 2016 US Presidential Elections, Facebook exposed data on up to 87 million Facebook users to a researcher who worked at Cambridge Analytica, which worked for the Trump campaign. The campaign team used this information as a micro-targeting technique, displaying customized messages about Trump to different US voters on various digital platforms.[34] For example, the collected data was specifically used by "Make America Number 1 Super PAC " to attack the Democrat candidate Hilary Clinton through constructed advertisements that accused Clinton of corruption as a way of propping up Donald Trump as a better candidate for the presidency.[35]

Manipulation of personal data and opinions using various social media platforms is another way governmental organizations can invade the privacy of social media users. Interactions with the government on social media thus result in bias and breach of the protection of personal data. Even without deliberate misuse, the intentional goal underlying media technology is to extract as much attention from its users as possible. Leveraging tremendous amounts of data, algorithms behind YouTube recommendations and Instagram reels target opinions to the people like young adults who are most susceptible to them and governmental bodies can easily manipulate and use these data to their benefit.[36]

When asked what the government could do to better protect data privacy of citizens, a respondent said, "Taking appropriate steps to improve and reinforce a Cybercrime unit in the Police would go a long way towards digital safety. Ensuring Cyber Security Awareness sessions in schools, or arranging for such sessions by trained professionals." Current trends show that Police cybercrime units of many states use private stakeholders to solve cybercrime cases and lack of professionals in cybercrime cells. Most young adults according to the survey don't know the proper means to access help when faced with cyber security threats.

Another opinion was, "There should be a comprehensive cybersecurity programme in all schools, that is mandatory and accessible to all." Currently, even though the NEP 2020 emphasizes on teaching technical

[33] Reuters, 2022, Twitter seeks judicial review of Indian orders to take down content -source | Reuters
[34] Vox, 2017, The Facebook and Cambridge Analytica scandal, explained with a simple diagram - Vox
[35] CNBC, 2017, Here's everything you need to know about the Cambridge Analytica scandal
[36] Center for Humane Technology (https://www.humanetech.com/)
Aryan, The Economic Times, 2022 https://m.economictimes.com/tech/technology/educational-apps-indulged-in-practices-that-put-childrens-privacy-at-risk-report/articleshow/91893218.cms

subjects like artificial intelligence or cybersecurity, no proper courses on cyber safety have been introduced in any higher educational institutions or school curriculum

6.4 Interactions with EdTech

The Indian Government's National Education Policy, 2020 came at an opportune moment, providing momentum to the EdTech sector. It stressed the development of EdTech infrastructure and specifically envisaged the establishment of the National Educational Technology Forum, a platform for the free exchange of ideas on technology in education.[37] One of the major names in the industry is BYJU'S that has made a big impact on the online learning world since its launch in 2015. The India-based mobile learning app, created by Byju Raveendran—a teacher by choice and entrepreneur by chance—is now used by more than 15 million students and has 900,000 paying subscribers.

Education is one of the main reasons why young adults access social media or the internet in general. According to the survey, the majority of the young mass uses their online presence for educational purposes, may it be having online classes, online coaching, exam preparation, self study help or just for satiating their learning curiosity.

Potential Threats

According to a Human Rights Watch (HRW) report, the pandemic pushed a large boom in the EdTech scene. Millions tune in each day through educational apps and websites to have access to education online. But there are severe data breaches in these online systems which puts data of minors at risk. Educational apps and websites run by the government as well as private entities of the 49 most populous countries indulged in practices that put children's privacy and safety in danger.[38]

In an Indian context, HRW analyzed apps such as Diksha, an initiative of the National Council of Educational Research and Training (NCERT) which is run and managed by the Ministry of Education, the e-Pathshala app, which is also managed by the NCERT, as well as privately run online education institutions like Khan Academy, Smart Q, and Top Parent. These apps, according to the analysis, indulged in practices such as collecting the identity of devices used to gain access to these apps or websites using data fingerprinting, collecting precise location data, and installing software development kits inbuilt into the systems which collect information for advertising. HRW report also stated that these apps did not allow the users, mostly children, the option to deny their data being shared with a third party.

In September 2020, it was reported that due to a server misuse and malpractice at EduReka, the personal data of more than 2 million users was publicly exposed, including details about their age, sex, phone numbers, and their parents' details. Such data breaches put the users, majority of whom are minors, at risk. These days breaches can be misused to be targeted by malicious hackers, lured into financial scams, targeted by exploitative advertising, and personal harassment.

EdTech platforms may also use the personal data of their users that they collect for internal business planning purposes - to track traffic, user engagement etc., for targeted marketing and at times, share it with associated or

[37] Arora and Mendiratta, 2021, Need for data protection framework for Edtech sector
[38] Aryan, Economic Times, 2021, Educational apps indulged in practices that put children's privacy at risk: report - The Economic Times

partnering entities to position their product or services to prospective customers. This data could also be used for targeted marketing specially on social media.

7. Analysing Social Media Platforms

Privacy policies can be defined as "terms of use" and legalities that lay out the procedure, conditions, liabilities and limitations involved with the use of a social media platform or any other online platform. The main aim of privacy policies is to protect the data of users and make them aware of what they should expect on the platform, and ways in which they can control how their data is used/shared. In recent years, there has been a storm around privacy policies of widely popular social media platforms, one of the main reasons being, lack of clarity.

When asked about data collection patterns of social media platforms, Mr. Avneesh Saluja from Netflix shared that it varied depending upon their purpose. "Google, Facebook etc collect different data than Netflix, because they need consumption patterns for advertisement. Netflix does not make money from advertising, so we collect data that helps give recommendations and increase user activity," he said.

7.1 WhatsApp

Features and Privacy Policy[39]

Whatsapp, a part of Meta Platforms, is one of the most widely used messaging platforms out there. It would be difficult to find even a single person in India with a smartphone who does not use or know about WhatsApp. Not only in India, but WhatsApp has also become a household name in several parts of the world. It is exactly its widespread usage that makes it even more important to examine its policies to protect the data privacy of its users.

One of the most widely supported and primary features of Whatsapp is its "end-to-end encryption." This means that no one apart from the two conversing parties, not even WhatsApp can see or listen in to what is going on in the chat unless one of the users reports the chat.[40]

Disappearing messages (that allows users to control how long messages stay in the chat), the ability to delete a message within one hour of sending it, and the option of allowing any media to be viewed only once are also data privacy-friendly options available to users.

Whatsapp also has status privacy, messaging privacy, and "last seen" privacy controls among others that allow users to significantly control and decide how much of their data to share

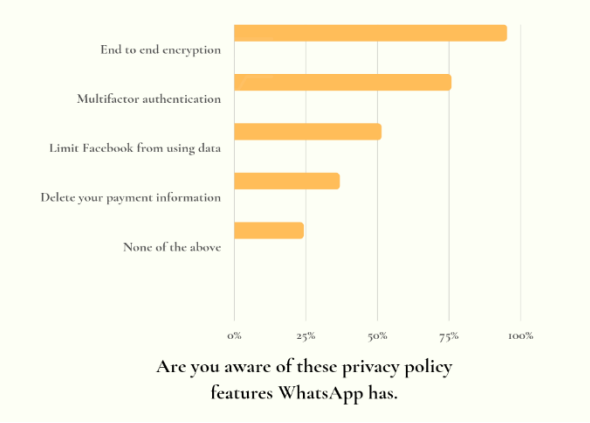


Fig 5: As per the survey conducted by us, we found that 25% of respondents don't read the privacy policy.

[39] Meta Co., WhatsApp, https://www.whatsapp.com/legal/?lang=e
Gaurav Arora and Raghav Mendiratta, Times of India, timesofindia.indiatimes.com/blogs/voices/need-for-data-protection-framework-for-edtech-sector/
[40] Aashish Aryan, Economic Times, 2022, m.economictimes.com/tech/technology/educational-apps-indulged-in-practices-that-put-childrens-privacy-at-risk-report/articleshow/91893218.cms.

with contacts on WhatsApp and who can message them/add them to groups.

Whatsapp Business is also fast becoming a platform used by businesses, big and small alike, to connect with buyers and advertise their products. This brings in another set of users in the scenario. Now conversation is not just between two or more parties who know each or connect due to work purposes. It is now possible that there will be monetary transactions on whatsapp itself, made even more convenient by the recent "Payments" feature on Whatsapp. A different set of policy governs such transactions. Whatsapp also explicitly states that they do not store payment details of users in their database.

Whatsapp also has a very detailed policy on "Legal Use" of Whatsapp Services and "Harm to Whatsapp or our users."

Gaps

Whatsapp's "Terms of Service" state, *"We analyze how you make use of WhatsApp, in order to improve our Services, including helping businesses who use WhatsApp measure the effectiveness and distribution of their services and messages. WhatsApp uses the information it has and also works with partners, service providers, and affiliated companies to do this."*

While this tells the users that their WhatsApp behavioral patterns are being analysed by the system to provide a "better user experience," there is no specification as to what information exactly is being collected, how it is being analysed and who are the parties with access to it. Interestingly, many other platforms have a clause with similar language without specifications.

Whatsapp Business Policy states, "*We provide, and always strive to improve, ways for you and businesses and other organizations, to communicate with each other using our Services, such as through order, transaction, and appointment information, delivery and shipping notifications, product and service updates, and marketing.*"

However, there is no section specifically stating what kind of information is stored, whether it is available only to Whatsapp or also to affiliated businesses as well. There is also no clarity as to when and how, if at all, this stored data is deleted. It is similarly possible to find other gaps in a deeper examination of policies. Moreover, the language in certain areas involves legal complexities, making it difficult for a lay person to comprehend.

7.2 Instagram

Features and Privacy Policy

Instagram, owned by parent company Meta Platforms (formerly Facebook Inc.), is one of the world's most popular social networking services. Individuals of varied ages across the nation have access to Instagram and use the app to share photos and videos with friends and colleagues, as well as strangers.

Instagram too follows "end-to-end encryption", ensuring that from the moment a message leaves your device, it is illegible until it reaches the receiver's device. This means that nobody during this process, including Meta Platforms itself, can see or listen to any messages. "Vanish mode" offered on all chats on Instagram DMs also

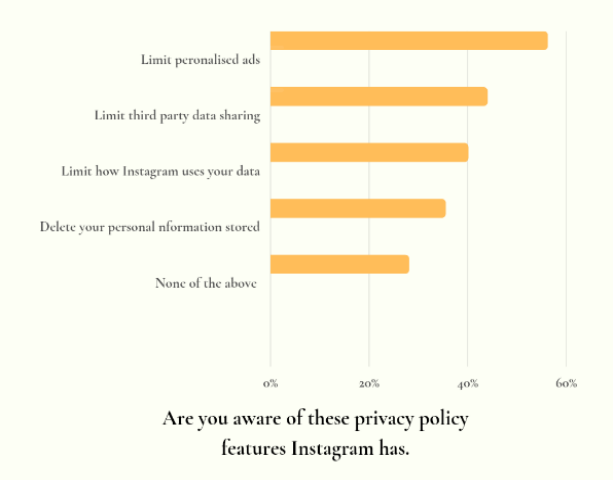


Fig 6: As per our survey about 30% of users are not aware of any of the Instagram privacy features.

adds an extra layer of privacy to users. When turned on, both the sender and the receiver can view messages sent only until they exit the chat. Once the chat has been closed, the messages have as rightly named, "vanished".

Additionally, Instagram offers features to streamline who can see what data. "Stories" have viewer counts with the ability to restrict people's access to your data. Accounts can be made private or public depending on the user, with private users having the opportunity to allow specific users to view their profiles. Instagram also allows accounts to be public or private, depending on the user's preferences. Private accounts ensure that any and all followers are approved by the user before having access to their profile. Both public and private accounts have the option to remove followers and/or block anyone. [41]

Gaps

Instagram's data policy states, *"We collect the content, communications and other information you provide when you use our Products, including when you sign up for an account, create or share content and message or communicate with others. This can include information in or about the content that you provide (e.g. metadata), such as the location of a photo or the date a file was created. It can also include what you see through features that we provide, such as our camera, so we can do things such as suggest masks and filters that you might like, or give you tips on using camera formats."*[42]

This policy, while theoretically correct and accurate, is extremely vague, especially from a non-professional audience. The usage of the word "can" makes the user assume that the collection of information is only when required, while on the contrary, this data is collected all the time. It also establishes the fact that the location and time frame of a file is not the only data that is being collected - to suggest personalized features, the company requires much more specific data.

Instagram's privacy policy also states, *"The information we collect and process about you depends on how you use our products. For example, we collect different information if you sell furniture on Marketplace than if you post a reel on Instagram. When you use our products, we collect some information about you."*

Avneesh Saluja, from Netflix USA, explained that Instagram collects data to help create user-related advertisements for a higher revenue. Since Instagram is a majorly free platform, there is no other way for the company to make a revenue. The data that is collected is sometimes encrypted, but is sold between companies for a greater advantage. However, companies have gotten more competitive about their data, and are proving to sell lesser data across companies.

Young adults are aware of the different measures that they can take to protect their data from being collected and secure their personal data from misuse and malpractice by social media platforms. **79%** of survey

[41] Instagram, https://help.instagram.com/116024195217477
[42] https://help.instagram.com/519522125107875/?helpref=uf_share

respondents stated that their Instagram accounts are private and **20.95%** said that they have restricted how strangers view their stories. **58.06%** don't allow strangers to follow them on Instagram and thus have established the first barrier against privacy breach. **53.76%** of respondents shared that they don't interact with Instagram personalised ads and **61.29%** of respondents shared that they don't give their personal information to these companies even if they do interact. When it comes to WhatsApp, **49.46%** of responses said that they don't share their WhatsApp registered phone number with anyone they don't personally know. Even though they are aware and take the measures necessary, many still neglect the minute details through which their data privacy can be violated like by accepting cookies (**30.11%** of respondents shared they accept all cookies) or by not reading the Privacy Policy and just accepting it in one click (**34.41%** of respondents shared they never read the privacy policy). Privacy policies of social media platforms can have loopholes through which data can be collected and accessed by third parties which is a major concern for data privacy. The policies thus need a vigorous revision to make them more secure, robust and accessible.

8. Introducing the Data Protection Bill

The current Data Protection system in the country is not comprehensively codified. When asked about remedies available to Indian citizens for data privacy breaches currently, Mr. Ruhail Choudhury, Corporate Lawyer and one of our stakeholders, said, *"The IT act and IPC and CrPC provides legal provisions to deal with cyber crimes too, but considering the fact that our criminal laws are vintage and are very old therefore several important forward looking amendments in such laws are immediately required."*

In response to the rise of tech-based businesses and the threats young adults face online, the Indian Parliament had undertaken an exercise to formulate India's data protection regime in 2019 through the proposed PDP Bill. The Joint Parliamentary Committee Report on the Personal Data Protection Bill was published on December 16 2021. The revised bill is yet to be introduced in the Parliament. For the scope of the paper, we are discussing only the proposed age of consent and its implications.

For the bill, "personal data" is defined as any data about or relating to a natural person who is directly or indirectly identifiable. As an extension to the original draft of the bill, the revised version includes "non-personal" data. This effectively means that any data, including anonymized data, falls under the scope of this bill. Any entity that determines the purpose of processing such personal and non-personal data is termed a "data fiduciary". This includes the state, social media companies, e-businesses, etc[43].

According to the bill, any individual below the age of 18 years would have to obtain consent from their parent/guardian(s) in all cases of their personal and non-personal data being processed by data fiduciaries[44]. Further, the bill places a blanket ban on any automated processing of personal data to evaluate aspects relating to an individual, including profiling based on all premises.

8.1 Pros

A fine of Rs. 15 crores or 4% of the annual turnover is demanded of any data fiduciary found in violation of the bill. Further, an annual data audit is required to be conducted by all data fiduciaries. A Data Protection Authority will monitor the enforcement of related laws. Consequently, the bill is expected to grant and protect the right to

[43] Trilegal, 2021 (The Data Protection Bill, 2021 - Trilegal)
[44] Iyer, Bharti, 2022 (Data protection Bill puts Indian children at a disadvantage. Here's how - The Economic Times)

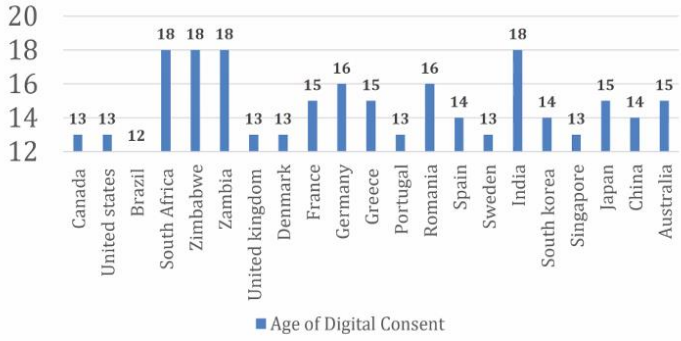
seek confirmation about any data processed by a certain company, to make changes to data collected for correction purposes, and to not have their data stored by data fiduciaries after the withdrawal of explicit consent. A secondary benefit of this bill is the projection of India as a nation with a strong data privacy regime. This reputation of the nation is intended to boost global trust and incentivise investment in the country.

8.2 Gaps

Despite these promises, the bill has been criticized for not taking into account the standard of "best interests of the child" that is otherwise adopted by Indian lawmakers when it comes to policies regarding the welfare of children. The restriction of access to the internet may put Indian children at a comparative disadvantage to their international peers, by inhibiting children's use of the internet as a medium of education, growth and self-expression. The widespread use of platforms like Unacademy, Vedantu, and BYJU's within the young adult community is indicative of the importance of complementary online education for Indian children.

Platforms or businesses who operate commercial websites / online services directed at children; or process large volumes of personal data of children will be notified as 'Guardian Data Fiduciaries' once the PDP Bill is enacted. Such 'Guardian Data Fiduciaries' are barred from undertaking activities such as profiling, tracking, behavioural monitoring, or targeting advertising directed at children, or any form of processing that could cause significant harm to children. The bill thus would cause a major tweak in the business model of a lot of EdTech companies, complicating access to education for a large proportion of Indian children.

Table 1: Comparative age of digital consent across jurisdictions



Beyond education, the internet offers healthy space and support to minorities like young adults identifying as LGBTQIA+. Platforms like Reddit and Discord offer communities for individuals to identify with and develop a strong network of support and security, components essential for adolescent growth. The bill threatens to completely deny access to such self-expression to young adults whose parents/guardians may not support their identity. This can leave young minds feeling suffocated within their offline communities and families with no apparent way out.

The rift between young adults and their parents can manifest itself in more ways about the bill. Although the bill shifts the responsibility of privacy from children to their parents, older people may not necessarily be in a position to understand digital privacy any better than young adults. Young adults themselves are exponentially more informed about social media and the amenities the internet offers, while many parents tend to incorporate a lot of conservative bias when thinking about these matters.

8.3 What We Think

It is clear from these anticipated consequences that the Data Protection Bill, although aiming to improve the well-being and privacy of children and young adults, gives rise to a plethora of other issues infringing on their freedom and growth. Ritesh Pandey, a member of the Lok Sabha, has suggested that to mitigate the unintended

consequences of the bill, the age of digital consent be reduced to 14 years. This is a suggestion taken from studying the ages of digital consent across other counties.

An alternate solution, as suggested by Manish Tewari, yet another member of the Lok Sabha, is to regulate data fiduciaries based on the type of content they provide or data they collect, as opposed to a blanket ban[45]. Fiduciaries like BYJU's and Unacademy, for example, may not be included in the bill, or may have separate, more appropriate age restrictions, since they provide educational content. Further, certain types of data, as for the purpose of regulating cyberbullying, may be excluded from the bill since the collection of this data contributes to the well-being of young adults.

9. Solutions and Our Recommendations

9.1 Recommendations for the Government (Policy Recommendations)

A. Re-evaluate the need for parental consent for digital activities under the age of 18

There can be no doubt that in this day, age and time, Young Adults are not only the most digitally empowered, but they are probably also the most digitally aware. We must not forget that these students have been through a period of "study from home" on a large scale, something that was beyond general public knowledge. Moreover, this generation has grown up with technology and the digital world being a very important part of their lives, thus, there must be cultivated trust in them, for them to know how to use social media to the optimum for their development. Moreover, requiring continuous parental consent might block off avenues of support for young adults- for instance, those belonging to the LGBTQ+ community and unable to converse with parents regarding their problems, and push them into a worse place emotionally. In fact, in most cases, parents might be less digitally literate than their children, and putting this power in their hands might end up limiting the child's personal development.

B. Create a policy framework for accountability and prevents abuse of power

Even though under the Right to Privacy in Article 21 of the Indian Constitution, government needs to follow a proper legal procedure before procuring any data from any data fiduciary but loopholes in the IT Rules, in the proposed PDP Bill and the frequent usage of the trump card of "threat to national security" has been used too often to infringe privacy of the citizens and the government to have access to any data they want. Indian laws for protection of data in such cases are too volatile unlike in the US where the government needs to go through a highly sophisticated procedure before having access to personal data. Microsoft in its policy mentions "If a government wants customer data – including for national security purposes – it needs to follow the applicable legal process. All of these requests are explicitly reviewed by Microsoft's compliance team, who ensure the requests are valid, and reject those that are not."[46] India needs a better data protection law that also stipulates the incumbent party from abusing power to their own whims.

[45] Mohandas, Kundu, 2022 (Nothing to Kid About – Children's Data Under the New Data Protection Bill)
[46] Microsoft, 2013, Responding to government legal demands for customer data - Microsoft On the Issues

C. Create a policy framework that is transparent and protects citizens, social media platforms and businesses alike

Social media platforms need to have better protection under law from falling under unfair legal action. In June 2020, Twitter India had to accept legal orders from the government to takedown "anti-national" content from their platform in an immediate manner. Twitter was warned by the IT ministry of criminal proceedings if it did not comply with some orders. Twitter complied to this so as not to lose liability exemptions available as a host of content. Such abuse of power by the executive body of the government needs to be resisted using the introduction of laws and policies to protect social media platforms which the public uses as a spot for free expression and help these platforms to adhere to their privacy policy and protect personal data of citizens without the fear of consequences.

Moreover, data on Young Adults, students and other citizens are also collected by state governments across India. It is here that the Right to Information under the Right to Life guaranteed in the constitution needs to be brought into play, as the citizens have the right to know when their personal information is being accessed by the State and how it is being used.

D. Minimize the risk of "function creep"

Data privacy frameworks, including the new Data Privacy Bill, proposed in 2019 (through its sections 12, 35, and 36) provide an exemption to the government. This creates a risk of “function creep”, whereby the personal data is used for other public functions (e.g. surveillance) beyond the originally intended or specified purpose. This risk is aggravated when there does not exist specific legislative authorisation setting out the purpose for which the personal data should be used. Thus, the data privacy law should aim to be extremely specific in its provisions.

E. Weave in considerations of evolving capacity and differential access in Young Adults

In the U.K., the age appropriation policies ensure that online services and platforms directed toward teenagers under the age of 18 follow certain guidelines (turning off geolocation, restriction on nudge features etc) to ensure greater data protection without prohibiting access. In India too, such a model can be considered. Not every 17-year-old sees, understands or perceives the world in the same way, or has the same level of maturity. The same goes for any other Young Adult. Requiring parental consent for all digital activities for all under 18 without considering unique differences and evolving capacities might end up restricting access to opportunities and do more harm than good.

F. Directions to social media platforms and online services (businesses, institutions etc) to honor the right to freedom of rest and leisure

Most of these social media platforms are built around the concept of "Echo Chambers." This means that they analyze what kind of content the user subscribes to and keep showing similar content continuously leading the user to become attached to the platform or even addicted. On the other hand, this also affects the diversity of opinion as we get stuck in the same circle. Thus, the new data privacy bill should direct the social media platforms to decrease the intensity of this system/algorithms so that users can naturally take time away from social media for recuperation, leisure, or increased productivity. The Right to freedom of rest and leisure is actually a part of the United Nations Universal Declaration of Human Rights

and thus will be in accordance with India's policy of incorporating International law within its domestic framework.

G. Give more importance and consideration to stakeholder opinions

Conversations with stakeholders- for example, lawyers, NGOs, subject matter experts, civil society organizations, academicians, researchers, etc- are important aspects in the primacy stage of policy making. However, it has been seen in the New Data Privacy Bill proposed by the Indian Parliament in 2019 that it included several clauses that have been criticized by these stakeholders. Considering the opinions and suggestions of these stakeholders in a more detailed and proper manner might lead to the creation of a more comprehensive and acceptable Data Privacy law working truly in the interest of the common people.

This requires considering the process of policy making. Usually after a bill is proposed, Joint or Standing Parliamentary committees are constituted to do a deeper dive into the bill and understand what the gaps are and how it can be made better. It is also at this point that stakeholder consultations are carried out to get varied/ diverse opinions on the matter at hand. What is important is to give more weight to the insights that emerge from these conversations while finalizing the bill, revising the structure, or including fresh clauses if required.

H. Introduction of Digital Literacy and Online Safety in curriculum

NEP 2022 does have provisions for educating students about online safety and digital literacy. In US K-12 schools and school districts, a digital citizenship curriculum is taught to students, India on the same steps should also include subjects like internet awareness and cybersecurity in its curriculum. Not only should the basics of digital literacy be covered, but also awareness around redressal mechanisms and data privacy should be encompassed.

9.2. Recommendations for IFF and Civil Society Organizations

A. Involve students in the process of formation of a data privacy law in India

Students are one of the primary stakeholders who will be affected by such a law. Thus, their opinions should matter in this regard and they should be allowed adequate representation. However, one thing to keep in mind is that students from marginalized communities might be unrepresented, which is a situation that should be avoided. Moreover, there is a possibility that the suggestions from students might not be feasible or well-rounded due to their lack of experience, and provisions need to be made to accommodate the same.

At the same time, it is not possible for governmental organisations to reach out to students across social sections to gauge their opinions. Thus, organisations like IFF could consider carrying out large scale surveys and conversations with students to assess awareness, needs and opinions around their right to privacy and then make recommendations to the government. Since many of these organisations would also be grassroots organisations, they would have a better understanding of regional and social differences and take them into account while surveying students for a more comprehensive result.

B. Setting up of Digital literacy campaigns clubs

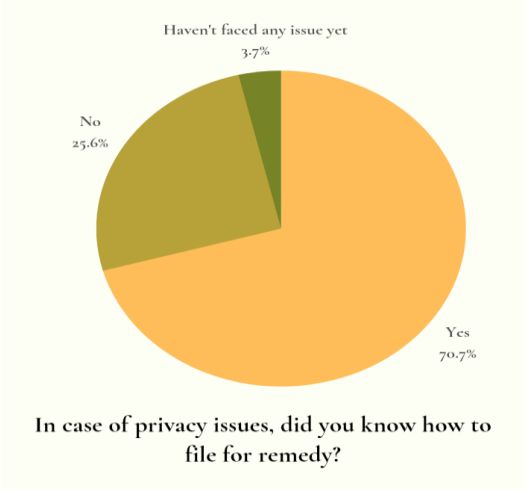


Figure 7: 70.7% Young Adults don't know how to file for remedy in case of privacy issues

School curriculum lacks in teaching young adults how to use the internet safely. Internet safety teaching is limited to discussion about viruses and hackers, while threats online extend beyond that. This results in lack of general awareness about what to do when faced with a cyber security threat. According to survey data, most young adults don't know how to file for remedy when faced with threats online.

NGOs and Civil society organizations that focus on digital empowerment and internet awareness should set up collaborations with schools to conduct proper Digital Literacy campaigns or set up clubs to educate young adults about privacy. Based on the framework and structure of YLAC and Oxfam India's Equality Clubs in schools, digital literacy clubs can educate students about how to use the internet safely, what are the threats online and how to have access to help when faced with cyber security threats. These clubs can also be leveraged to advocate for better privacy for young adults across.

C. Encourage advocacy and generate awareness

Awareness is the first step towards advocacy, and consequently, action. Civil society organizations and NGOs should create and disseminate material regarding issues of digital privacy in local languages to improve accessibility and promote greater understanding among people regarding these issues. This can also generate will among them to advocate for privacy issues that matter to ensure that their data is protected online.

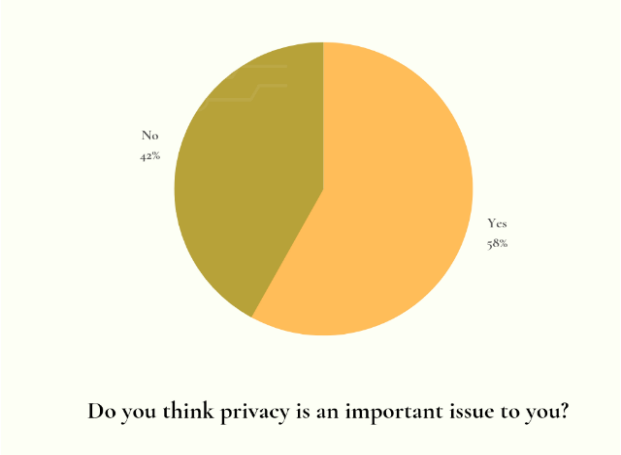


Figure 8: 58% Young Adults say Privacy is important to them (Primary Data)

When asked about what various organisations can do to promote digital privacy and safety internally, Valentina Raman and Zineb Mouhyi, Directors at YouthxYouth, a youth Education Activism organisation, said, *"It is very unrealistic to think at in this day and age your data will not be found online, no matter how much you protect it. Because that is, in fact, the job of some people- to find data. However, when it comes to ensuring data privacy within an organisation, there are two sides. One, you can create rules and policies and try to impose them on everyone and get them to follow it. Two, you can create a work culture where a space naturally develops where people are less likely to face this kind of abuse. This requires building trust and understanding each other. We at YxY tend to focus more on the latter because it proves to be more effective."*

9.3 Recommendations for Businesses and Social Media Platforms

A. Consider making privacy policies more accessible

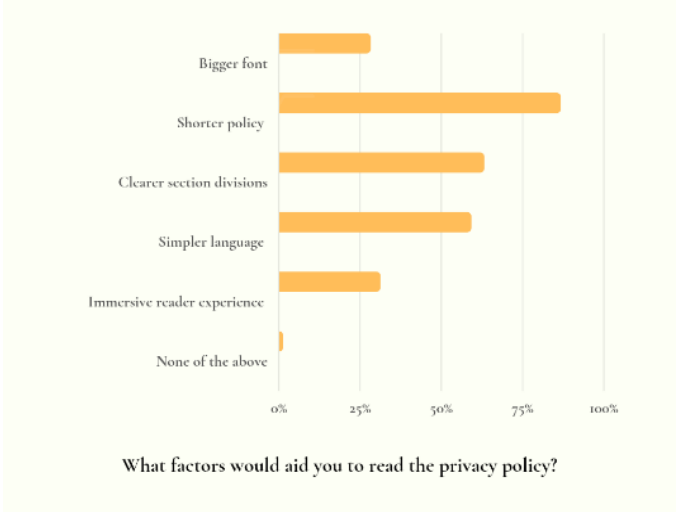


Figure 9: How to make privacy policies more accessible? Respondents speak (Primary Data)

Most social media platforms, including those that are widely used, have privacy policies encompassing thousands of words and complex legal language that is very difficult for most common people to understand or read patiently. This is one of the primary reasons why most Young Adults tend to click "Agree" before properly understanding what is being asked of them by the platform.

The top reason for not reading the privacy policy according to users, was it being "***Too long***," followed by being "***Too difficult to understand***." Thus, some steps that social media platforms and businesses online can do to make their policies more accessible would be to keep them precise and simplify the legalities wherever possible. They can also make their policies available in regional languages, and enable the "immersive reader" (audio+text) feature, which would make it simpler for individuals with reading barriers to access the policy.

B. More clarity in privacy policies

Most social media platforms share that certain data of users is shared with "affiliated partners" or "integrated partners," for a "better user experience," but there is no clarity as to which and how many partners it is shared with and what it is actually used for. Spelling it out for the users might make them feel safer about their data and trust the platforms more.

C. Pop-up Privacy policy feature

While users might not want to read an entire 16-20 page privacy policy at one go, we can surely spare 1-2 minutes now and then to eat a few lines of it, as our survey says that 58% of Young Adults do care about Privacy. Thus, social media platforms could consider adding a system wherein a small pop-up appears whenever users try a new feature, to mention in short the privacy features/policies associated with the use of that particular feature. For example, when a user starts an Instagram live for the first time, the pop-up could tell them about the terms of use for Instagram live specifically. Over time, this can help users become more aware of the Privacy Policy of the platform in general.

D. Data Minimisation

Social media platforms and businesses online should consider adopting/developing features and practices that minimise the amount of user data that is collected, instead of pushing them to provide more

data. This is also one of the practices outlined in the GDPR[47] adopted by the European Union in 2018[48]. Mr. Syed Kazi from Digital Empowerment Foundation, which has been working in the field of digital safety for over 20 years said, *"We collect only the absolutely required data from our members. If you don't collect unnecessary data, there will be lesser data privacy violations you need to worry about.*

10. Overall Limitations

The time frame for the research project was quite limited (about a month) so even more in-depth research could not be carried out.

Conversations with more stakeholders might have revealed more insights. (Other potential stakeholders listed in annex.)

The sample size is moderate. A larger sample size might have sparked deeper insight into the issue of privacy from the view of Young Adults.

The literature review is limited, so all aspects of the existing body of knowledge could not be covered.

Each recommendation comes with certain limitations which are covered within the scope of that recommendation.

11. Conclusion

In conclusion, we believe that it is imperative for young adults to be more aware as well as safer online. One of the first ways this situation can be greatly improved is by the government implementing a strong, comprehensive law to help protect data of the citizens. Young adults use social media for all sorts of interactions, having a majority of their lives in the online space especially after the horrors of a global pandemic. Both WhatsApp and Instagram, social media platforms we delved deeper into, have implemented multiple features to keep data secure and private. However, there is much room for improvement. We also believe that young adults should have control over their own data, rather than being required to be of legal age before being able to decide what they would like to share.

According to our survey data analysis, most young adults are aware of the ways in which their privacy can be violated on social media platforms and also do take precautionary measures to prevent such threats.

However, just awareness is not enough, action to better protect data privacy of Young Adults online is the urgent need of the hour. This can only be achieved through advocacy, and the government, civil society organizations, social media platforms, business and citizens working together to create a balance in the best interest of all.

[47] General Data Protection Regulation
[48] Burgess, 2020 (https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018)

12. Appendix 1: Survey

Survey Questions

13. Annexures

1. Potential Stakeholders for further detailed consultations:

A. NGOs:

- Digital Rights Foundation, Lahore
- Digital Rights Watch, Melbourne
- European Digital Rights Institute (EDRi)

B. Government Organisations:

- Digital India Corporation

C. Social Media/EdTech/Gaming

- Employees of Metaverse
- Employees of Indian EdTech platforms: BYJUS or Unacademy
- Employees of a public listed gaming company/ gaming company

2. Choice of Case Studies

In the "Interactions with Government", two case studies have been explicitly discussed. In the Indian context, the case study of Disha A. Ravi vs Union of India has been explained to provide an explanation of how the digital privacy of young adults can be violated by abuse of power by the Government. Disha Ravi was 22 years old when she was arrested and according to our survey's purview fell under the category of young adult. In an international context, the case study of the Cambridge Analytica Scandal has been discussed to provide an explanation of how manipulation of data can happen by the government. The idea behind discussing this case study is to show that manipulation of data can affect anyone who uses social media platforms no matter what their age as any ads can pop up in front of you due to the algorithm. Investigations have also shown that among the 87 million users affected by the scandal, data of the majority of young adults were exposed. The discussion of these two particular case studies were done to analyse the connection between governmental Interactions and breach of user privacy through that in the context of young adults.

14. Advocacy Material: Link to Open Access Design
