DigitalRightsFoundation
"KNOW YOUR RIGHTS"

YOUNG PEOPLE & PRIVACY IN ONLINE SPACES

ABOUT

Digital Rights Foundation (DRF) is a feminist, not-for-profit organisation based in Pakistan working on digital freedoms since 2013. DRF envisions a place where all people, especially women and gender minorities, can exercise their right of expression without being threatened. DRF believes that a free internet with access to information and impeccable privacy policies can create safe online spaces for not only women but the world at large

Contact information:

info@digitalrightsfoundation.pk
www.digitalrightsfoundation.pk

ACKNOWLEDGEMENTS

This study is an important part of the discourse DRF hopes to create in Pakistan around the sphere of digital rights and would not have been possible without the efforts of the DRF team and the direction of our academic consultant Dr. Maryam Mustafa.

DRF would also like to acknowledge the support provided by Privacy International.

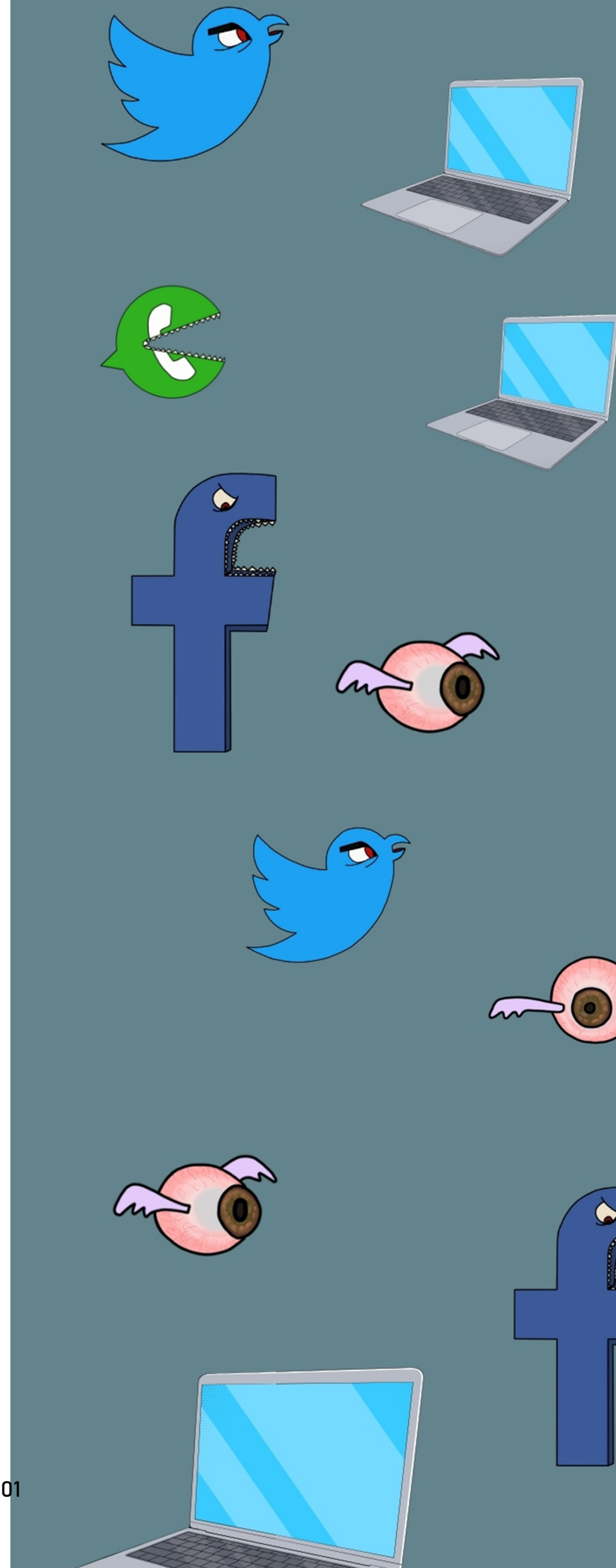
TABLE OF CONTENTS

INTRODUCTION

The understanding of privacy as a concept is widely absent in Pakistan, much of which is owed to the cultural impact of how and who we deem worthy of allowing the space to retain their privacy. There is the obvious gendered difference in how folks experience this Constitutionally-granted right due to archaic notions of propriety that come into play in a patriarchally structured society like Pakistan; however there is also a generational and seniority-based impact on the individual's expectation and realization of this right.

In the context of Pakistan both joint and nuclear families, in the way they are structured, afford little privacy to children, seen in the way their possessions such as bags, diaries, mobile phones are not considered off-limits by parents and can be monitored by them at will. Due to prevailing cultural norms, there is no clear concept of stepping into adulthood and thus gaining a certain amount of autonomy and independence, this pattern can continue well into the 20s and 30s for most individuals as the family structure, mode of living and living space tend to remain the same.

As more and more digitization takes place and the boundaries between the online and offline seem to be getting blurrier, the transition of offline behaviors seeping into online spaces and how young individuals utilize them and what control they exert over their gadgets that connect them to these spaces and their profiles themselves, is the focus of this study.



OBJECTIVES

The objective with this study is to take a deep-dive into the use and experience of online technologies by young individuals to gain a better understanding of the specific impact and challenges they are facing, in order to better address them in terms of advocacy. We hope to provide recommendations that will be used by policy makers to create a better and safer internet for our youth.

This study is operating on the hypothesis that children/young individuals face multiple challenges in terms of their online and data safety, on both an individual, platform and governmental level and that their privacy is impacted negatively as a result.

METHODOLOGY AND STRUCTURE

The data for this study has been collected through using group and individual interviews as well as an online survey. We conducted 8 in-depth interviews, including one focus group discussion. We also included 22 survey responses, data from which has been included in this study. That makes a total of 30 respondents between the ages of 13 and 18.

Finally, data from the questionnaire and interviews was compiled and analyzed. The insights from these findings are provided in this report and supported by a literature review. The report will begin with a literature review, followed by the findings gleaned from the surveys and interviews and end with a list of recommendations for multiple stakeholders.

POSITIONALITY

It must be noted that this study does not claim to capture the experiences of all young individuals across Pakistan. It does not assert that respondents are representative of the entire demographic of individuals living in Pakistan. In particular, though the participants came from some of the major cities in Lahore, Baloch and Pashtun representation was severely lacking. Additionally, participants mostly came from middle to upper class households and went to private schools. Indeed, there are experiences in terms of the right to privacy that are not represented in this original data. Therefore, to make generalizable inferences based on the data set would be an error. Furthermore, due to the ongoing COVID-19 pandemic, data-gathering was hindered due to limited availability of participants, virtual education and its scattered and time-consuming nature, inability to perform close field-work and internet connectivity problems. With a greater data set and increased respondents, the findings may be substantiated and strengthened further.

LITERATURE REVIEW

It is uncontroversial to suggest that our daily lives are inextricably and irreversibly linked to data in this day and age. From using credit cards to tweeting, we interact with data and technology on a daily basis. It would be naïve to think that these actions exist only in the moment we carry them out. In reality, every action forms the basis of our digital self: an avatar of us that lives online and reflects our likes and dislikes, ranging from our political opinions to where we like to shop. Ultimately, our right to privacy becomes threatened when we are not the sole owners of such data. It has only been two years since it was revealed that Cambridge Analytica was illegally harvesting data from millions of people through Facebook for political advertising.[1] Since then, privacy has been at the forefront of human rights concerns over technology. According to Raso et al, privacy is the single most impacted right by current AI implementation.[2] In the case of Facebook, Cambridge Analytica used personal details about people without their knowledge or consent. Not only is this a grave violation of privacy, it illustrates the extent to which personal data has become a central currency in the digital age.

As smartphone and internet connectivity penetration increases at a staggering rate, people from the Global South are becoming internet users.[3] As these communities come online, they appropriate technology that was not designed for them. Therefore, they face privacy challenges particular to them, highlighted by Ahmed et al and Sambasivan et al.[4] Ahmed et al reveal the privacy tensions in families in Bangladesh and study how an individual's privacy is compromised in family and commercial settings because of cultural expectations.

Individuals negotiate privacy by using software solutions, and social solutions such as blackmailing, negotiation and mutual agreements on usage. Sambasivan et al extend the understanding on privacy by studying the gendered use of technology in South Asia and highlight how the concept of privacy as understood by the 'West' frequently breaks down in other contexts.[5] In their study, they they reveal the complexities of how privacy breakdowns because of the shared (between, for instance, parent and child) and mediated usage of devices (by, for example, a husband teaching his wife how to use an app). Taken together, these studies underscore the need to understand the perception of privacy as it is situated in its context. This study is part of this tradition of understanding how privacy is perceived.

Article 14 (1) of the Constitution of Pakistan promises individuals the right to privacy, but as the concept of online privacy evolves, the legal instruments needed to implement and protect this right in the digital arena lose their teeth. Currently, more than 80 countries have laws to ensure and protect users' privacy and protection of their digital data. Pakistan is not among these countries.[6] Indeed, advancements in digital technology has led to greater efficiency in the delivery of many services and communication channels. However, with the growing digitalisation of services such as online payments, banking and records of identification, the lack of transparency and accountability in these records raises issues of privacy.[7] This is true of both private data collection and government owned databases. For instance, in May 2020, two massive data breaches led to the information of 115 million mobile subscribers being leaked online, including their names, national identification or CNIC numbers and addresses.[8] In December 2020, Pakistan's National Database and Registration Authority (NADRA) refused to accept responsibility for a data breach that compromised the data of over 100 million mobile users.[9] These incidents are one of many that represent the sensitivity and fragility of data usage in Pakistan, the lack of mechanisms in place to protect and track data use in the country, and the precarious nature of privacy as it exists in the digital age in Pakistan.

In this climate of endangered data privacy, one of the most vulnerable groups continues to be young people and minors. According to a report by UNICEF, 1 in 3 internet users is a child, and there are not enough mechanisms in place to protect them from the dangers of the digital arena.[10]

The internet provides opportunities for young people to share and express their opinions, communicate with others and learn the essential skills of digital literacy needed in today's world. The internet also increases accessibility of information for disadvantaged and underprivileged young people who would otherwise be confined by limited resources in the physical world. However, with these opportunities comes the perils of online spaces. As previously discussed, the dangers of misuse of data, harmful and dangerous content, surveillance and online abuse increase by several folds when children are involved. UNICEF's report specifies that children are also at risk of more explicit forms of violence such as exploitation, abuse, addiction, trafficking and online child sexual abuse.[11]

Such findings beg the question of how young people are engaging with tech and online spaces, and more pertinently, how they perceive their own online privacy.

Findings from around the world suggest that young people and children are becoming digitally literate and more aware of their privacy, but in selective ways. For example, Zhao et al found that children under 11 were able to identify and articulate privacy risks such as information oversharing or revealing real identities very well. Alternatively, they were less aware of risks such as online tracking and game promotions (and things like autoplay).[12] Tufekci found that most youth are less disturbed by abstract invasions of privacy by government agencies and corporations than the very real and ever-present experience of trying to negotiate privacy in light of nosy parents, teachers, siblings, and peers.[13] Corroborating this, Madden et al has found that teens are sharing more information about themselves today on social media sites than they did in the past. Moreover, teen users do not express a high level of concern about third party access to their data.[14] However, in a study by Marwick and boyd, they found that American teenagers placed significant emphasis on "trust and respect" a marker of whether they would share private information online.[15] These understanding of technology is not uniform--while they are well-informed in some instances, they nonetheless, continue to be vulnerable to online harms.

A 2020 report by UNICEF focused on the experiences of 301 children across four countries in East Asia and found that 2/5 children had bad experiences they would not want to tell anyone about. This was true of both boys and girls who reported receiving sexually lewd photographs from strangers online.[16] Additionally, Willoughby identified several areas of risk involved in young people's use of social media, which included cyberbullying and online abuse as well as exposure to negative forms of user-generated content.[17] These findings suggest that privacy breaches and online harms are common risks faced by young people in online spaces.

In addition to these dangers, young people also faced privacy breaches and harms from their own peers and users online. For example, in a cross-country analysis, Burton and Byrne found that children of an increasingly younger age were going online, and all children surveyed were accessing disturbing content such as adult pornography, violent images and suicide sites. However, what seemed to bother them most was when other children post or say hurtful things about them, hate speech and discrimination.[18] Mitchell and Jones, using the Youth Internet Safety Survey in 2005, found that in the US, almost one in three youth reported harassing someone online at least once in the previous year. Similarly, of the 129 youth who reported using the Internet to harass or embarrass someone, 81% said that someone else did it to the respondent first.[19] In Canada, Johnson et al found that four in ten teens (42%) had shared a sext with someone else. 39% of senders of sexts stated that their sexts had been further shared with or forwarded to someone else in person without their consent, thus violating their privacy as it was reserved only for the sole intended recipient.[20]

Young people also display a range of complex strategies to counter and negotiate through privacy concerns in online spaces. This includes

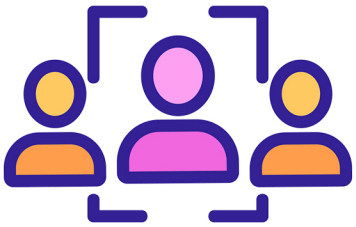
ways in which they articulate their own priorities in the digital space, which we have already discussed. In addition, it involves the protection tactics and strategies they adopt to secure themselves against online harms.

Marwick and boyd investigated the ways in which teenagers conceptualised privacy and found that many engaged in tactics to regulate who could access their information online. This went beyond regular individualised sense of privacy towards what they referred to as "networked privacy" where privacy is conceptualised as a system of ever evolving networks and requires ongoing negotiations. With this understanding, Marwin and boyd noted that a common approach is to ignore the technical features of social media altogether and instead focus on encoding the content itself in order to limit the audience. By encoding their content in plain sight, teenagers limited their content to those that understood their codes and could interpret them, such as close friends, and hid it from those they didn't, such as parents.[21] This pattern of encoding is also found in the Twitter subculture of 'subtweeting' where non-confrontational tweets are used to address specific individuals for whom they are made. To an ordinary user, these tweets may appear vague and mundane. However, to those aware of the context, and therefore the 'codes', they become gateways to accessing personal sentiments and opinions of the user who creates them.[22] In this way, young people achieved privacy without using the necessary mechanisms in place, such as privacy settings on social media platforms, to ensure their safety. As Marwick and boyd note in the case of 'networked privacy', these techniques and strategies are ever evolving as those networks and relations in the digital spaces change.[23]

Given these findings, this report investigates the ways in which young people in Pakistan, including teenagers and minors, understand and conceptualise privacy. This includes interrogating whether they see it as important, what they consider to be breaches of privacy and what impact such harms have on them. In addition, this research looks at the various strategies young people have adopted to negotiate boundaries in online spaces, including the protection tactics they have embraced in order to secure themselves online. There is limited research on the privacy of young people in Pakistan. Khalid conducted a study in 2017 on the impact of social networks on Pakistani students and found that a majority of students (71%) reported not being aware of the terms and conditions of social networking sites.[24] Beyond this, studies into the privacy-related concerns of young people online are scarce.

FINDINGS

a. Participant demographics



The study involved responses from 30 individuals mapping their experiences of being in online spaces. Of those 30, 22 identified as female while 8 were male. 14 respondents were from Lahore, while another 7 were from various cities in the Punjab province. 9 respondents were in Karachi while 1 was from Hyderabad. Another respondent was a Pakistani based in Dammam, Saudi Arabia. Every single respondent was a cell phone user. While a majority (18) also used laptops, a few also mentioned additional devices such as PCs and tablets. 18 respondents said they shared some devices while using others, presumably cellphones, as personal devices. Most used WiFi services to connect to online spaces while a limited number of people used a combination of 4G and WiFi.

A large majority of the participants stated that they were using social media as a communicative tool, networking and socialising tool. Others noted using social media for entertainment, gaining news and meeting new people. 22 participants stated having private accounts with the exception of 6 participants who reported having a combination of public and private settings on various platforms. Only two participants noted having completely public accounts. Most notably, 13 participants stated that they had been using social media when they were under the age of 13, which is how old you need to be in order to make an account. The youngest age noted was 6 years old.

b.perceptions of privacy

All participants agreed that privacy was important to them and an integral part of their online experiences. Several suggested that they prioritized privacy over all other aspects of their online existence. They equated privacy with things such as safety, including drawing offline parallels between being private online and being in the safety of their own homes.

> "If I didn't have privacy then I would go crazy um so I feel like privacy is something that is a requirement for me. Otherwise then, if there was no privacy then it would just be, like, really horrible on the internet especially. So I feel like privacy is a necessity for me." - P2

Another respondent drew distinctions between the public and private realm, viewing privacy rights through the lens of a 'boundary' that separates the private from the public:

> "To me privacy is like, having a boundary you know? between you and the outer world and everything, and privacy is also being able to control who can see, like who can enter that boundary and like you know. Privacy for me is just like, you know, being in your house with your family, just knowing nothing bad is going to happen to you."

The safety gained from online privacy also came from the comfort of knowing that those with access to the users' personal information were people they knew in real life. This idea was inextricably linked to ideas of trust, which many participants emboldened in their responses.

"I am more comfortable because I know the people that are going to be looking and I know there's not going to be anyone that's going to be looking at my pictures but like with bad intentions" -P1

"You don't have permission to, agar unhon ne aap ko bheja hai aap kisi aur ko agay na bhejo [if they have sent it to you, you should not send it forward to someone else] because they sent it to you for a reason and they - because they trust you and you break that trust." - P4

"If I'm trusting someone with something it's basically that you don't have to screenshot it" -P6

Several participants, including women, highlighted the particular importance of privacy in online spaces for women. This was reflected in the examples they gave of privacy violations, which were often around leaked information, including sensitive pictures and gendered impact such breaches had.

c. offline parallels

Drawing parallels between offline and online spaces was a recurrent theme in most responses. Participants often articulated the importance of privacy and their perceptions of privacy breaches and violations through drawing connections to their offline lives.

"Even in person when you tell a friend a secret or like when you are talking to a friend and that friend goes and tells some-one else that's like a break of your privacy right." -P1

"It's like, you know, like when you're sit-ting in a car and a random person makes eye contact with you" -P1 [when talking about what it means to have your privacy invaded]

"Because if you're threatening someone in real life, I'm pretty sure there's gonna be some negative reaction" - P2

"Within the span of one month I kind of no-ticed seven different dramas right and it's like school may have shut down but like that aspect of school hasn't really you know shut down entirely" - P7

In addition, young people who were students also stated that they relied on online spaces to stay connected in their offline lives. For example, several students mentioned having to join Facebook social groups in order to gain membership into school societies. In the same way, others mentioned having online feuds amongst friends transpire into offline arguments in school. Participants reported using the 'block' and 'report' mechanism on social media platforms against those they were fighting with in schools, and using their offline networks to direct social media attacks on others. Alternatively, such tactics were also used to protect them from online abuse. Some stated that they counter online harms by asking their friends in real life for support against such attacks. This theme will be discussed later in the chapter.

d. online harms

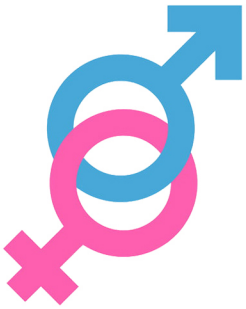
Privacy violations experienced ranged from doxing, hacking to saving a picture posted by someone else. A notable harm mentioned often was the leaking of pictures and others gaining access to private information about oneself. Participants were particularly alarmed by what others may do with their private information once a breach had occurred. For example, several young people noted being afraid of being blackmailed by others and their school peers finding out private information about them. In addition, terms like 'invasive', 'invasion' and 'exposed' were often used to denote actions associated with privacy breaches. Privacy, in contrast, was synonymised with safety and trust, as mentioned. Participants corroborated this dichotomy by mentioning instances where lack of privacy had led to online violence against them.

"The message requests section is horrible people leave all sorts of nasty comments there and add you to group chats where they share disturbing images" -P22

"It's importance because if everything about you leaks online, it can get in the wrong hands and can be exploited for wrong purposes or with the intention of harming you" - P25

"Private lifestyles and habits that you don't really want out there that keep getting exposed" -P7

e. gendered harms



Several of the female respondents recounted incidents involving gendered digital harms. Gendered digital harms can refer to a harm caused in the online sphere due to someone's gender. In Pakistan, this is a particularly common occurrence as social media is considered a public domain. Therefore, women are often treated the same as they are in public, through combinations of moral policing, shaming and controlling behaviour in an effort to curtail their public presence and expression. In fact, the layer of anonymity and lack of accountability afforded to individuals allows them to be more explicit and overt in inflicting gendered harms.

Female respondents, as well as some of their male counterparts, acknowledged that women's experiences of the online domain was markedly different to those of men. In particular, younger females reported being harassed online by men more frequently, including being repeatedly inboxed and being sent lewd photographs. Notably, several female respondents reported being followed and approached by older men. Male respondents, contrastingly, reported being 'catfished'[25] by other men pretending to be female users.

"Growing up I realized some people have followed me like older men and older people that follow me, realizing what they're intentions were just made me more made me want to be more private in my life because I just realized the type of people they were, you know?" - P1

"He was just commenting again and again on all of my stories and how and why I post stuff and I just didn't feel safe so I just blocked him." - P4

"Once someone sent me a picture if their private parts (male)" - P29

"I have female friends who get message requests on FB and Instagram, so they do block people. For boys, I think it's less but there are fake accounts acting as a girl. So yes, I have blocked accounts but for females, I think it happens comparatively more" -P8

f. impact of online harms and privacy breaches

Several users also mentioned the impact online harms and violations of their privacy have had on them. Some recalled lingering feelings of insecurity and continued fear of online spaces.

> "I feel like because I had public accounts those posts will always be out there like someone might have taken a screenshot or might have whatever. But they're always going to be public which is why I feel like I still am public" - P1

> "I always have this lingering fear keep the second i'm online as a second because something can happen to me i don't think there's a safe place on the internet" - P7

One person recalled having their private thoughts revealed by their close friend publicly on social media. They noted that this resulted in a major backlash in both online spaces through abuse and social ostracisation in offline spaces, causing them to have anxiety and paranoia for several months following the incident. This was representative of a major theme of mistrust in online communities and anxiety as a result of online interactions.

> "I'm like i'm gonna get violated my stuff's gonna be used in the wrong way i'm gonna end up somewhere"- P6

> "I am monitored 24x7 while I'm on the internet right so i think being connected to the internet itself gives you potential privacy intrusions and attacks. I don't think anybody should feel truly safe on the internet. You think you're safe behind like an anonymous username and an anonymous account but really you're not. You're never safe on the internet" - P7

g. strategies

In line with findings from Marwick and Boyd's the conceptualisation of privacy, the young people interviewed displayed a wide range of new strategies to protect themselves from breaches of privacy and online harms. This includes preventative measures as well as coping mechanisms after faced with online negativity. Respondents noted using traditional routes, such as the 'report' and 'block' mechanisms on social media frequently, particularly when faced with negativity online such as hacking and hate speech.

> "I do end up blocking people that I do not necessarily cannot handle anymore there's only so much click you know pressure and p from a single person I can take" - P7

In addition to traditional routes, young people also employ collective forms of solidarity in online spaces to protect themselves.

"I told one of my friends I'm like hey yo, you know how to do the [inaudible] again I'm like I need your help it's like he helped me he he pulled a few strings and like I got my account back so like I guess I have friends for that and connections" - P6

"If someone is harassing or something then i can just like you know put them in a group chat my friends you know like troll them just like you make fun of them or whatever" - P1

Friends were also a major source of security and vetting for strangers. For example, young people displayed a reluctance to give out phone numbers, but did express an interest in meeting new people on social media. As such, they were more forthcoming with their social media usernames because of an added sense of security. In this way, social media was considered more secure than giving out phone numbers. This may be because friends were thought to add an added sense of privacy.

"Nowadays nobody gives their numbers because people just put numbers on washroom walls and stuff so like when you have to pick up someone, you ask for their insta, you never ask for their number." - P3

"I asked my friends' friends' friends' friends whether they are chill people and so yeah, I knew. And also I met them with a friend." - P3 [on meeting someone they had spoken to online]

"I would tell my friends so then they spread the word about how much of a bad person this person is." - P2

h. rejected protection tactics

Notably, there were two frequently rejected protection tactics among young people online. Firstly, when given a hypothetical situation in which they were faced with an alarming privacy violation, few minors stated that they would talk to or tell their parents. Again, for several of them, their first point of contact was their friends. In fact, most young people said they would actively avoid telling their parents for fear of misunderstanding or negative repercussions for them, not the offenders. As a way to avoid parental involvement in their activities, they also acknowledged blocking or limited what their parents could see. Other tactics included creating alternative accounts for just their close friends.

"If i told my mother, she would feel like that these things are really dangerous and she would probably close my account so i would talk to someone else about it maybe like my sister or my best friend" -P5

"If I post a meme about me being suicidal my mom's gonna get me checked to the therapist or something. I'm gonna go straight there so like I had to learn to like uh I guess restrict or block some people in my family" - P6

"I personally wouldn't complain to a school supervisor or parent, I would try to get rid of the page or like you know report it on Instagram" - P8

In addition to these rejected tactics, participants displayed relatively little knowledge or belief in authorities. Many participants were aware of international standards and bodies that govern digital affairs, but stated that they were unaware of any online-specific laws in Pakistan, such as the 2016 Prevention of Electronic Crimes Act. Despite understanding that online harms such as hacking and doxxing were violations, they did not believe that Pakistan had any legislation to criminalise such behaviour. In addition, when given the option of approaching institutional bodies such as the FIA's Cyber Crime Wing or relevant police authorities, most displayed reluctance to approach relevant authorities. This not only suggests that young people are uninformed about measures for redress, but that they also perceive these institutions to be ineffective in countering online abuse and privacy violations.

"I don't know where to go for like harassment purposes, so I'd probably just report their account and then tell everyone to report their account to get it removed" - P3

"One of my friends did report to FIA but they didn't really respond to him. And even if they did, it was 2 or 3 months later. In Pakistan, the authorities aren't that responsive on these issue" - P8

"I report or block them but I don't know any legal and more effective procedure" - P24

Additionally, respondents also alluded to a lack of belief in social media platforms, suggesting that though they prefer in-platform reporting to be the primary course of action, they do not have much confidence in it either. Some stated that reporting did not remove the content in time, while others stated that reporting only made the content more visible.

"Even when you report something, it's there for three days or four days, even if you catch the person" -P8

"I have reported posts and accounts that were seemingly disturbing, or inappropriate. But nothing was done against it" - P13

"Most social media platforms don't take anything seriously and online matters only become worse." - P13

"[I] would probably report and ask my close friends to do the same but it's not likely that it will get removed or deleted or someone's account being banned because it has never worked before." - P18

In conclusion, young people gave privacy in the digital space a significant amount of importance in their lives, going so far as to say they would consider leaving social media if their privacy was violated or revoked. They equated privacy concerns with issues of trust and safety, relating those themes back to their offline lives. For instance, participants considered privacy violations similar to being watched or harmed in public. They also placed a significant emphasis on their offline lives in school, including their education and social lives, having an impact on their online presence and privacy online. Young people expressed concern over several forms of online harms, including cyberbullying, hacking, and doxxing. Female participants in particular showed concern for gendered harms such as being sent lewd pictures and being harassed by older men and having their private information shared with others. The impact of online harms and privacy breaches was wide ranging, from mental health concerns to the limiting of social media presence and usage. As such, participants also shared some of the strategies they had adopted to

protect themselves and negotiate better spaces for themselves online. These included using existing mechanisms such as 'blocking' and 'reporting' but also mobilising their offline connections, such as close friends to counter the harms in the online space. Notably, children expressed hesitance to completely block someone without first questioning them and also resisted telling parents or family members about their concerns for fear of negative consequences towards them.

RECOMMENDATIONS

Based on our findings presented above, we discuss the below recommendations on designing for privacy in our context and populations.

FEEDBACK FROM PARTICIPANTS

The young people involved in this study were asked two questions that have informed this section. The first question asked them what would make them feel safer in online spaces personally, and the second question asked what they felt were changes necessary to online spaces, in general. Their responses, taken together, form the basis for this particular section. Responses ranged from institutional change to social and personal development.

A. Digital literacy

Participants suggested that there needed to be more education in the realm of the online sphere. They complained of not being given enough information regarding online spaces, including how to be safe on the internet. Female respondents also suggested that women should be given additional training on digital safety because they are more vulnerable to online abuse and harm. Overall, more commitment to digital literacy in the context of growing digitalisation in Pakistan was a primary suggestion. This could be done through intervention at the school level, through additions such as digital literacy classes to the existing curriculum. Alternatively, social media companies could introduce basic training through tools such as audiovisual tutorials for younger audiences when they are joining social media. Civil society organisations could also provide dedicated training to young people in collaboration with schools.

B. Social media platform responsibility

Given the lack of belief in social media platforms' ability to address online harms and risks, many young people had no suggestions because they did not feel they would be implemented. Of those that did suggest changes, the primary recommendation was better content regulation, including more rigorous monitoring of harmful content and quicker response times to reporting mechanisms. In addition, others suggested that newer privacy policies should be included such as limiting viewership of posts to 'Close Friends' on Instagram, in the same way it allows for Instagram Stories.

A frequent complaint from participants was that they were being harassed online by strangers, often those not in their age group. For those who were online to find new friends and network with others, vetting strangers was difficult due to unregulated age specifications on social media. Therefore, accidentally adding grown adults to their social networks was considered a major privacy breach that participants feared. In order to secure themselves from this harm, participants suggested additional vetting mechanisms for social media platforms. For example, one participant suggested that only those individuals who are in the same age range should appear in one's 'Suggested Friends' list. Another stated that there should be a "personality questionnaire" before anyone joins social media so that only like minded individuals are suggested as friends.

The researchers note here that while this is a valid suggestion based on the vantage point of the participants, there would be some concerns with enforcing it. Primarily, the requirement this would place on users to give up additional personal information and the added justification it would provide social media platforms to mine user's data further would be reasons why we are hesitant in condoning this line of thought.

C. Social change

Another frequent suggestion came from participants who said that responsibility did not lie with social media platforms but with society as a whole. They stated that the problem of online harms was not rooted in social media itself, but in human behaviour, which sees lack of accountability and transparency as a way to instigate violence online, as it is offline. Therefore, in order to reduce online harm and ensure privacy in the digital arena, change must be enacted at the root of the issue, which is social relations. This is particularly pertinent given the issues of gendered harms, which are rooted in systemic misogyny at a societal level. As previously noted, women's public presence is often considered reason enough to direct abuse against them, so to counter this harm directly would require intervention at the socialisation level, to normalise the idea of women taking up space in public spaces, including digital ones.

General recommendations

It is important to note for all the recommendations laid out here for different sectors, that a paternalistic approach to regulating online spaces for young people must be avoided. A paternalistic structure by its nature requires a less progressive approach and views those it seeks to safeguard, such as children and young people, as passive subjects. As demonstrated by this research, young people are autonomous individuals with rights, desires and a nuanced understanding of technology and online spaces. Given the legal status of young people, i.e. below the age of majority, there is always the temptation to negate their understanding of their experiences and seek to "protect" young individuals without empowering them through structures such as surveillance and control which recreate many of the power dynamics that result in lack of safety in the first place.

For the state

- Introduce school curriculums that include digital literacy in schools that provides children and young adults with the ability to stay informed, engaged, and safe online.
- Introduce gender sensitisation content into curriculum and at an early age, to combat gender stereotyping and the related thought process that leads to online gender-based violence.
- Digital citizenship, i.e the use of technology to engage with society, politics, and government, is a vital concept that should be taught in the classroom. It could explore multiple avenues of digital citizenship including digital ethics and anti-harassment discourse. Linking concepts of consent with technologies is important to teach young people how boundaries and safety translate online.
- Investing in public-private partnerships to develop programs and educational campaigns on issues of privacy, safety, and digital rights.

For schools

- Rethink their policies on traditional harms that occur between peers to include the translation of offline harms into online violence and vice versa.
- Policies on handling non-traditional harms such as those occurring the digital domain need to be given dedicated attention and intervention in the appropriate manner, including educating students on cyberbullying.
- Schools need to work in collaboration with parents to understand what forms of intervention are necessary to counter digital harms. This includes determining where it is the responsibility of the school and where parents need to intervene.
- Consider the risks of cyberbullying and lack of accountability in the context of the ongoing COVID 19 pandemic and online schooling.
- Introduce sessions on the potential harms in online spaces for parents. In particular, those focusing on privacy features and ways and means to keep children safe while maintaining their privacy.
- Providing and investing in resources such as judgment-free counseling to students experiencing online harassment and bullying.

For civil society actors

- A clearer understanding of the issues faced by young people will allow for a more focused and specific form of advocacy for their rights in digital spaces. Thus, more time and effort must be directed to studying this sphere in Pakistan's context.
- More collaboration between digital rights and child rights organisations to develop coalitions and advocacy based on shared understanding.
- Lobbying with the relevant State departments and institutions to be especially cognizant of the personal data protection rights of minors. It is an urgent and important point to be pressed with the Ministry of IT as we are on the precipice of launching our data protection law.
- Lobbying with the relevant authorities and State to implement through the law and in terms of policies, the international covenants, conventions, and obligations that Pakistan is a signatory to and has ratified, such as the Convention on the Rights of the Child (CRC).

For social media platforms

- The language and design of privacy features sections need to be reworked to become more friendly and accessible to younger audiences. Alternatively, there need to be separate audio visual tutorials or briefs designed for younger audiences to educate them about specific privacy features and their options.

- Short, accessible video/audio training on privacy features, community guidelines, potential harms and how to stay safe before signing up to the platform should be introduced for young people.

- Understanding cultural and linguistic complications tied to the violations faced by young people online. Much of the hateful and violent content posted online is in languages other than English, and therefore, take longer to report and remove. More must be done to ensure that all forms of disturbing content in all languages are being treated with the same urgency.

- Introduce contextualized policies and content moderation mechanisms that are responsive to local languages and politics. More resources for human moderators for the local context, with safeguards in place to ensure the safety and wellbeing of content moderators, i.e. living wages, humane workload and resources to prevent traumatisation.

- Contextualised privacy prompts designed for women and gender minorities to remind them (at the time of posting) who is able to view their images, information. In particular, this would be salient where images are tagged with their specific locations.

- More transparency regarding the use of data, and those who are able to view user data.

- Developing transparent and speedy mechanisms of reporting and taking down child sexual abuse material from social media platforms, as well as transparent and human rights complaint methods of sharing data on such matters with local law enforcement agencies.

- Working with local civil society organisations to map areas of concern and empowering them with access to data and information to become watchdogs.

- A more refined, contextualised, and clear pathway to reporting, especially maintaining the anonymity and privacy of the complainant.

CONCLUSION

Our findings suggest that there is a growing involvement of young people in online spaces. With the rise of apps such as TikTok and Instagram, young people are a crucial part of the digital arena. However, young people's participation in online spaces comes with little protection and security being offered to them in Pakistan. In particular, young people display little knowledge about their rights in online spaces or the mechanisms that exist in the country to protect them from online harms. Nonetheless, minors place great value on their privacy and online security and do not shy away from using measures such as reporting and blocking to counter online harms. Additionally, both male and female users show an awareness of gendered harms and the asymmetry with which they are experienced disproportionately by women in digital spaces. Notably, the naturally evolving divide between younger and older people and the power dynamics within schools and families means that younger users are unlikely to approach their older counterparts when faced with privacy breaches but do employ intra-social group strategies to counter harms. Whether these strategies are enough to ensure complete protection for young people across Pakistan cannot be stated with confidence. Therefore, it is pertinent to ensure that the combined efforts of the state, civil society and society at large are mobilised to strengthen and implement legislation and mechanisms for the protection of young people.

BIBLIOGRAPHY

Ahmed, Syed Ishtiaque, Shion Guha, Mohammad Rashidujjaman Rifat, and Faysal Hossain Shezan. 2017. “Privacy Vulnerabilities in the Practices of Repairing Broken Digital Artifacts in Bangladesh” 13: 15.

Ahmed, Syed Ishtiaque, Romael Hoque, Shion Guha, Rashidujjaman Rifat, and Nicola Dell. 2017. “Privacy, Security, and Surveillance in the Global South: A Study of Biometric Mobile SIM Registration in Bangladesh.” Digital Privacy, 13.

Bahia, Kalvin, and Stefano Suardi. 2019. “The State of Mobile Internet Connectivity 2019.” GSMA Connected Society. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/07/GSMA-State-of-Mobile-Internet-Connectivity-Report-2019.pdf.

Baig, Asad. 2019. “Privacy in the Digital Age,” October 27, 2019. https://www.thenews.com.pk/tns/detail/568763-privacy-digital-age.

Byrne, Jasmina, and Patrick Burton. 2017. “Children as Internet Users: How Can Evidence Better Inform Policy Debate?” Journal of Cyber Policy 2 (1): 39–52. https://doi.org/10.1080/23738871.2017.1291698

Davies, Harry Davies. 2018. “Facebook Told Me It Would Act Swiftly on Data Misuse – in 2015 | Harry Davies.” The Guardian, March 26, 2018, sec. Opinion. http://www.theguardian.com/commentisfree/2018/mar/26/facebook-data-misuse-cambridge-analytica.

Hofstede, Geert. "The Cultural Relativity of the Quality of Life Concept." The Academy of Management Review 9, no. 3 (1984): 389-98. Accessed April 15, 2021.doi:10.2307/258280.

Hope, Alicia. 2020. “Information of Over 115 Million Pakistani Mobile Subscribers Exposed in a Massive Data Leak.” CPO Magazine, May 15, 2020. https://www.cpomagazine.com/cyber-security/information-of-over-115-million-pakistani-mobile-subscribers-exposed-in-a-massive-data-leak/.

Johnson, Matthew, Faye Mishna, Moses Okumu, and Joanne Daciuk. 2018. “Non-Consensual Sharing of Sexts: Behaviours and Attitudes of Canadian Youth.” MediaSmarts, 54.

Kamran, Hija. 2019. “Privacy-in-Law: How Safe Is Your Data?” Digital Rights Monitor (blog). September 27, 2019. https://www.digitalrightsmonitor.pk/privacy-in-law/.

Keeley, Brian, and Celine Little, eds. 2017. Children in a Digital World. The State of the World’s Children 2017. New York, NY: UNICEF.

Madden, Mary, Amanda Lenhart, Sandra Cortesi, Urs Gasser, Maeve Duggan, AAron Smith, and Beaton Meredith. 2013. “Teens, Social Media, and Privacy.” Pew Research Center: Internet, Science & Tech (blog). May 21, 2013. https://www.pewresearch.org/internet/2013/05/21/teens-social-media-and-privacy/.

Mansouri, Abad. 2020. “Sensitive Data of over 100m Pakistanis Breached; Interior Ministry, NADRA Deny Responsibility.” Digital Rights Monitor (blog). December 30, 2020. https://www.digitalrightsmonitor.pk/sensitive-data-of-over-100m-pakistanis-breached-interior-ministry-nadra-deny-responsibility/.

Marwick, Alice E, and danah boyd. 2014. “Networked Privacy: How Teenagers Negotiate Context in Social Media.” New Media & Society 16 (7): 1051–67. https://doi.org/10.1177/1461444814543995.

Mitchell, Kimberly J, and Lisa M Jones. 2012. "Youth Internet Safety Study (YISS): Methodology Report." Crimes against Children Research Center, 15. "Our Lives Online." n.d. Accessed April 23, 2021. https://www.unicef.org/eap/media/4691/file/Our%20lives%20online.pdf.

Raso, Filippo, Hannah Hilligoss, Vivek Krishnamurthy, Christopher Bavitz, and Kimberly Levin. 2018. "Artificial Intelligence & Human Rights: Opportunities & Risks," September. https://dash.harvard.edu/handle/1/38021439

Sambasivan, Nithya, Garen Checkley, Amna Batool, Nova Ahmed, David Nemer, Laura Sanely Gaytán-Lugo, Tara Matthews, Sunny Consolvo, and Elizabeth Churchill. 2018. "'Privacy Is Not for Me, It's for Those Rich Women': Performative Privacy Practices on Mobile Phones by Women in South Asia," 17.

"TRANSITION TO TWITTER: Teenagers Create a World of Subtweets and Slang." 2015. The Octagon. February 8, 2015. https://www.scdsoctagon.com/online-exclusives/features/2015/02/08/transition-to-twitter-teenagers-create-a-world-of-subtweets-and-slang/.

Tufekci, Zeynep. 2008. "Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites." Bulletin of Science, Technology & Society 28 (1): 20–36. https://doi.org/10.1177/0270467607311484.

UNICEF East Asia and the Pacific Regional Office and the Centre for Justice and Crime Prevention, Our Lives Online: Use of social media by children and adolescents in East Asia - opportunities, risks and harms, UNICEF, Bangkok, 2020

Willoughby, Mark. 2019. "A Review of the Risks Associated with Children and Young People's Social Media Use and the Implications for Social Work Practice." Journal of Social Work Practice 33 (2): 127–40. https://doi.org/10.1080/02650533.2018.1460587.

Zhao, Jun, Ge Wang, Carys Dally, Petr Slovak, Julian Edbrooke-Childs, Max Van Kleek, and Nigel Shadbolt. 2019. "`I Make up a Silly Name': Understanding Children's Perception of Privacy Risks Online." In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, 1–13. Glasgow Scotland Uk: ACM. https://doi.org/10.1145/3290605.3300336.

DigitalRightsFoundation

"KNOW YOUR RIGHTS"

www.digitalrightsfoundation.pk

info@digitalrightsfoundation.pk

DigitalRightsFoundation

DigitalRightsFoundation

DigitalRightsPK