Building a Safe and Inclusive Cyberspace for Women

Executive Summary

There exists a gender gap in digital literacy and access to Internet services in India due to reasons that include household and social controls restricting access to services offered by the Internet, ineffective legal redressal mechanisms and faulty content moderation guidelines developed by social media platforms to deal with online abuse and harassment. CyberPeace Foundation has been working extensively on building inclusive cyberspace by fostering cyber awareness amongst women, caregivers, children, mothers, and law enforcement authorities through our capacity building initiatives. We propose the following policy recommendations in this brief for the stakeholders involved -

- Build strong fallback mechanisms for women outside of their homes to facilitate reporting of online abuse and harassment accompanied with counselling sessions.
- Increase the frequency of focused trainings on cyber awareness with workshops on gender sensitization for law enforcement officials and men.
- Define the contours of online abuse and harassment to ensure it is narrowly tailored to reduce the existence of objectively offensive content on social media platforms.
- Facilitate reporting on cybercrime portal and on social media platforms by designing intuitive reporting mechanisms.

A presence in cyberspace provides opportunities for economic and social empowerment as it provides a platform to voice opinions, access resources, and conduct businesses.

1. Women for the purpose of this policy brief are people above the age of 18 who identify themselves as women on social media platforms. We understand women are not a homogenous group. Caste, class, religion, disabilities, geography and sexual orientation play a huge role in how women access services and are received on the Internet. To delimit the scope of the present policy brief, we decided to deal with intersectional aspects of online abuse and harassment in our second brief in the series of policy briefs on Building Safe and Inclusive Cyberspace for Women. The recommendations proposed in this brief are a result of primary research conducted by CyberPeace Foundation and insights collected as part of CyberPeace For Women campaign and panel discussion on Building Safe and Inclusive Cyberspace for Women.

What is the Policy Issue?

The utility of being digitally literate and having access to cyberspace was made evident during the COVID-19 pandemic in India when crowdsourcing of medical resources using social media platforms saved many lives. Despite internet access being patchy due to infrastructural roadblocks in most of India, there was a noticeable increase of nearly 46 million internet users from 2020 to 2021 as reported in the Digital 2021 April Global Statshot Report. The report also shared numbers that were reflective of the gender gap in access to internet services in India. Only 23.8% of the percentage of the ad-audience from Facebook is female, the rest being male.

Female presence on other social media platforms including YouTube (31.2%), LinkedIn (28.3%), Instagram (27%), Facebook Messenger (22%), Twitter (8%) remains to be abysmal except for Snapchat (40.6%) which is doing slightly better. We can not divorce experiences in cyberspace from those in the physical world, but situations get accentuated as the reaction time decreases significantly due to constant access and the probability of understanding expressions and intent of the people behind the screens decreases. Women in India are missing out on registering their presence on digital platforms and this excludes them from various opportunities of contributing to their as well as the country’s growth. The following are some of the pertinent reasons identified by CPF that would be addressed as part of the policy recommendations presented later in the document.

1. Household and Social Controls

While the cost of internet connectivity has decreased over the past few years, there is a 20% gap in ownership of mobile phones between men and women, according to GSMA 2020. Limits to the access of phones, laptops and in some cases, cybercafes, are set by men and elders of the household. They consider using phones indecent and want to ensure the safety of women on digital platforms as they are themselves unaware of how to safely access the platforms. These social controls cripple the confidence of women by instilling fear within them and feeding into the realization that if something were to happen they would not have access to readily available fallback mechanisms at home.

In our primary research studies on assessing cyber awareness in seven states, we found out that women find themselves at the risk of victim shaming if they report online abuse and harassment. This stigma is perpetuated by the aforementioned social controls. They also find themselves reluctant to go to police stations to report cybercrime.

2. Gaps in Digital Literacy

Along with the gap in access, there is also a divide in digital literacy amongst women. Digital literacy includes the skills required to utilise the opportunities afforded by the internet while staying safe. Most often women are unaware of the types of harms that are committed on social media platforms, the mechanisms provided by social media platforms to ensure their safety, the legal redressal mechanisms that are at their disposal and the skills that should be honed to ensure the safety of their data and their digital identities.

The Government of India had proposed three digital literacy programmes - The National Digital Literacy Mission 2014, The Digital Saksharta Abhiyan 2014, and the Pradhan Mantri Gramin Digital Saksharta Abhiyan. These schemes have not been able to deliver on the targets that had been

---

2. There were 1.39 billion internet users in India till January 2021.
3. The statistics are based on data collected from Facebook which as of now only captures the data on its male and female population.
4. Majority of the Indian population access internet services using their mobile phones as access to broadband services is sparse.
5. As part of CPF’s cyberawareness campaigns in eight states, namely Assam, Manipur, Rajasthan, Andhra Pradesh, Meghalaya, South West District of Delhi, and Punjab, CPF had conducted research studies to measure cyber awareness amongst citizens.
outlined in their proposals due to the lack of necessary budgetary allocations, overlap in the three schemes which complicate the monitoring processes and the outdated course objectives as the skills being taught are divorced from the digital experiences of citizens who prefer using smartphones to computers, among other issues.

3. Gaps in Legal Redressal Mechanisms

Most of the experts as part of our CyberPeace For Women campaign had recommended that we should add stricter and more specific provisions under Information Technology Act 2000 (IT Act) and Indian Penal Code to deal with cybercrime committed against women. The National Commission for Women has also conducted several stakeholder consultations with experts and representatives from social media platforms to address gaps in the legal redressal mechanisms by assigning stricter liability to social media intermediaries and penalties for perpetrators of cybercrime.

The Ministry of Electronics and Information Technology released the Information Technology (Guidelines For Intermediaries And Digital Media Ethics Code) Rules, 2021 (IT guidelines) to expedite the process of takedown of problematic content on social media platforms under Section 79 of the IT Act, in March 2021. While the guidelines aim to bolster online safety and reduce the spread of misinformation, the guidelines are over-inclusive in their identification of the categories of content that requires due diligence from platforms. The absence of this diligence will lead to platforms being held liable for penalties or losing safe harbour. For instance, social media platforms have to notify users if the content uploaded by them is “obscene, insulting or harassing on the basis of gender, racially or ethnically objectionable, or post that threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign States” and that it might lead to the removal of information or suspension of their account. IT Guidelines give the government similar unchecked control over content like the nullified Section 66A\(^6\) by criminalising speech through vague and over-inclusive standards of content removal.

Law enforcement authorities are also not adequately trained in comprehending the extent of cybercrime committed against women and in the tools along with the techniques that can be utilised for investigation. They continue to understand cyberspace as an extension of physical space devoid of its added complexities. They resist filing complaints as they do not understand the nature of the harm. To address this, the government had set up a cybercrime reporting portal to ease the process of reporting.

But the portal is often non-operational, categories of cybercrime are difficult to comprehend and follow-up to complaints happens rarely. Moreover, in cases where follow up does happen, action is not taken by the police officials.

4. Faulty Content Moderation Strategies adopted by Social media platforms

Additionally, social media platforms in their current form are neither inclusive nor safe for women. Due to their unequal presence, women are often fearful of online abuse and harassment that will be meted out to them. This fear has also been substantiated by newspaper reports, researches, and real-life incidents of cyber stalking by their previous partners or colleagues, incidents of Image-Based Sexual Abuse (IBSA) when they shared their number to donate plasma during the pandemic and so on, displaying the harsh reality. The reporting mechanisms on these platforms have been criticised for the delay in content takedown and inconsistency in the implementation of community guidelines for content moderation.

---

\(^6\) Section 66A of the Information Technology Act 2000 was struck down by the Supreme Court in Shreya Singhal vs Union of India, 2015 as the section penalised sending messages causing annoyance, inconvenience, danger, obstruction, insult, injury, and criminal intimidation. The judgement stated that the phrases used were too vague and criminalised speech protected under Article 19. But FIRs are still filled under the section to curb criticism of the ruling party.
Platforms have over time begun employing artificial intelligence tools to fasten the process of identifying problematic content. Unfortunately, it has not been successful in addressing a majority of problematic content in India due to a gap in contextual understanding of caste, and religious dynamics that play a part in how women’s position is identified in the society, along with comprehension of regional language which often leads to over and under-inclusive removal of content. The platforms also do not secure the privacy and security of women by design as they do not have intuitive reporting mechanisms. Unfortunately, these situations often lead to women censoring their views and even deleting their accounts voluntarily from all social media platforms and even deleting their accounts voluntarily from all social media platforms.

POLICY RECOMMENDATIONS

1. Building strong fallback mechanisms for victims and perpetrators

While there has been an incremental upsurge in reporting of cybercrimes, this data is not reflective of the number of cybercrime. It is thus imperative to build and strengthen a sustainable ecosystem for women to come forward and report crimes without hesitancy by building a fallback mechanism for them like the One Stop Center Scheme. In the absence of a readily available fallback mechanism at home, with the help of trained therapists, psychologists and lawyers, the victims would be assisted in reporting cybercrime and work through their trauma. This will assist in increasing reportage and ensure accountability of perpetrators. This will also provide the National Crime Records Bureau with updated data on the emerging kinds of cybercrime so that interventions can be developed by government stakeholders to address them.

7. We understand that the NCRB report is purposive in its understanding of crimes and motives of committing crimes but it is a good starting point to understand the psychology of cyber criminals.

2. Training and workshops on cyber awareness for all

The state with the assistance of NGOs should increase the frequency of trainings and workshops on types of cybercrime, investigation tools, reporting mechanisms, cyber hygiene, and legal redressal mechanisms with an increased focus on men and law enforcement officials. These trainings should have an additional component of gender sensitization. While NGOs and state bodies like the National Commission for Women have been conducting such trainings for women and children, it is equally important for men to be involved in them. In CPF’s trainings, we have spoken to quite a number of men who were unaware of the ramifications of their actions. This intervention would enhance the capacity of individuals to explore the opportunities provided by the internet while ensuring the safety and security of their data, digital identities and that of others. These trainings have to be backed by constant updation of training materials as the technology is evolving at a rapid speed.

3. Defining scope of online abuse and harassment

It is imperative for the state to outline the contours of online abuse, hate speech and online harassment to
remove ambiguity, vagueness and discretion on part of the law enforcement officials and social media platforms as we run the risk of violating the fundamental right to speech which is sacrosanct for a democracy. The laws should be narrowly tailored to deal with cybercrime that is objectively offensive like stalking using electronic media, IBSA and Non-Consensual Sharing of Intimate Images (NCSII) on priority. The community guidelines for content moderation should be based on the laws of India and should be context-specific to the interplay of identities in India. The platforms would have to meet these prerequisites due to the demographic and geographic advantage of the user base from India. AI systems employed by the social media platforms should be based on identifying the minimum threshold that meets the requirements outlined by Indian laws.

4. Design-based solutions to assist in reporting on social media platforms

Content reported by victims on social media platforms is evaluated if it violates community standards using algorithms or by overworked content moderators. There is also inconsistency across platforms on content moderation guidelines. For instance, Twitter allows for pornographic content to be uploaded on their platforms while Instagram does not allow it. Content, even if inappropriate, is often not taken down because it is not flagged under the right reason. Developing chatbots to assist in identifying appropriate categories based on the content moderation guidelines of a particular platform in regional languages would help in reporting under appropriate categories on social media platforms and cybercrime reporting portal. For instance, AI-driven Spot is a conversational interface for ensuring a safe workplace culture, which guides one through the process of flagging, by allowing them to input suspicious conversation and pulling up appropriate categories to report it under.

India presents a unique position due to its linguistic diversity and lack of digital literacy. Creating chatbots to assist intuitive reporting in local languages could help tackle this problem. In the short term, providing an example sentence for each reporting category could also help in reducing misreporting. Facebook, for example, already provides fact-checking services in ten regional languages. It can assist in providing the chatbot for reporting in these ten languages first. It is also imperative to include women in the development of such platforms to ensure the design of platforms is accommodative of the experiences of women and can preemptively come up with solutions to such recurring issues.

References

