INDIA FUTURE FOUNDATION
Freedom of Expression, Trust and Safety on the Internet

CHILD SAFETY NEWSLETTER

News From Around the World

IN THIS NEWSLETTER

News From Around the World ----------------------------01

Online Child Safety Policies Around The World---------------------------04

Interventions By States And The Private Sector In India-----08

Steps Taken By Different Stakeholders-----------------------11

CRY Report highlights increased risk of online sexual exploitation and abuse of children

According to a report published by Child Rights and You (CRY), a Non-Government Organization (NGO) working in the area of child rights, in collaboration with Chanakya National Law University (CNLU), a national law university based in Patna, Bihar, the COVID-19 pandemic heightened the risk of Online Sexual Exploitation and Abuse (OCSEA) towards children. The study found that the lockdown and the resultant movement of education services to the Internet had made children more vulnerable to online perpetrators. As per the findings of the study, adolescent girls and boys, in the lower income bracket, aged between 14-18 years, were the most vulnerable group.The report also revealed that 33% of the parents surveyed reported that strangers approached their children via online platforms, with most of them typically soliciting personal and family details and engaging with them in inappropriate sexual conversation.

Category A Abuse Represents 20% of Illegal Images of Child Sexual Abuse Material Online

According to a report by the Internet Watch Foundation (IWF), an NGO based in England working on making the Internet a safer space for children and adults, the most extreme form of Child Sexual Abuse Material (CSAM), known as Category A abuse, accounted for a fifth of such content found online, last year. The IWF, monitors the distribution of CSAM, and found more than 51,000 instances of Category A abuse, which includes imagery of rape, sadism, and bestiality. The report stated that the increase in Category A imagery, in 2022, was partly due to criminal sites selling videos and images of such abuse, with the number of webpages dedicated to making money off CSAM having more than doubled, since 2020. The IWF reported taking action on over 250,000 webpages last year, with three-quarters of them containing self-generated imagery, where the victim is manipulated into recording their own abuse before it is shared online.

The National Society for the Prevention of Cruelty to Children (NSPCC), a child protection charity, has stated that the figures are “incredibly concerning” and that the UK government must update the online safety bill to ensure senior managers are held liable for the presence of CSAM on their sites.

Under the Bill, tech executives face the threat of a two-year jail term for failing to protect children from online harms. However, the provision applies only to content such as material promoting self-harm and eating disorders, and does not apply to dealing with CSAM.

The security minister, Tom Tugendhat, had called for companies to use heavily encrypted services to build in safety features that help detect abuse. On the other hand companies such as WhatsApp have expressed concern about the provisions in the Bill that could force them to apply content moderation policies that would amount to circumventing end-to-end encryption. The IWF had stated that child sexual abuse content is being treated as a “commodity” on some sites, with criminals looking to exploit more and more insidious ways to profit from the abuse of children.

Paedophiles using VR headsets to access child abuse imagery in the UK, warns NSPCC

New figures obtained by the National Society for Prevention of Cruelty to Children (NSPCC), a children's charity in the UK working in the areas of child abuse, through a Freedom of Information request has revealed that paedophiles in the UK are using Virtual Reality (VR) headsets to view and store child abuse imagery. The charity obtained data from 45 police forces, in the UK, on the number of child abuse image offences and found that eight offences involved headsets and VR. The NSPCC is now warning that the growing use of VR to explore the so-called Metaverse, a variety of virtual games, chat rooms and experiences, is exposing children to new online risks.

As a result The NSPCC has urged the government to create a statutory child safety advocate through the Online Safety Bill. Social media or gaming sites were named in 9,888 offences, with Snapchat involved in 4,293 offences, Instagram in 1,363, Facebook in 1,361, and WhatsApp in 547. The NSPCC has warned that "unregulated social media is fuelling the unprecedented scale" of the problem.

The Online Safety Bill is currently being reviewed in the House of Lords, with VR headsets and the Metaverse covered by its provisions. The government has warned that companies failing to protect children may face huge fines and criminal sanctions against their senior managers.

While the VR figures are small compared to the overall picture, which saw a record 30,925 offences committed in the year 2021-22 involving possession and sharing of indecent images of children, the NSPCC argues that the figures are just the tip of the iceberg. The charity has reported that it hears from young people who feel powerless and let down as sexual abuse risks becoming normalised. The problem of using VR headsets for child exploitation has been raised since its inception, with commercial adult sex work already utilising the technology. The BBC first reported, in 2017, that VR headsets were being used to sexually exploit children. In 2022, the BBC reported that a Metaverse app allowed children to enter strip clubs.

Indian Government Exposed Personal Data of Students and Teachers Online for Over a Year

According to WIRED, the Indian government exposed the personal data of nearly 600,000 students and over a million teachers on the open web, for more than a year. The data included children's names, schools, locations, test scores and partially sensitive phone numbers and email addresses. The information was obtained through Diksha, an app owned by the Ministry of Education, Government of India, that provided online education to students from grades 1 to 12. Despite multiple letters from Human Rights Watch raising concerns, the Government of India failed to take action to protect children's privacy.

ONLINE CHILD SAFETY POLICIES AROUND THE WORLD

Protecting Children from Cybercrime: Indian Government Takes Action

The Government of India has implemented several measures to protect children from cybercrime, including the enactment of the Information Technology (IT) Act, 2000, which has provisions to deal with prevalent cybercrimes. Section 67B of the Act specifically provides for harsh punishment for dissemination, reading or transmitting of child pornography, in electronic form. Sections 354A and 354D of the Indian Penal Code provide for punishment for cyber harassment and cyber stalking against women.

The Protection of Children from Sexual Offences (POCSO) Act, 2012, is a crucial piece of legislation that specifically addresses sexual offences committed against children. POCSO criminalizes cybercrime against children, including child pornography, cyber stalking, cyber bullying, defamation, grooming, hacking, identity theft, online child trafficking, online extortion, sexual harassment and violation of privacy.

The government has also introduced the Personal Data Protection Bill, 2019, which seeks to protect the personal data of individuals and establish a data protection authority for the same. Chapter IV of the Bill provides for processing of personal data and sensitive personal data of children.

In addition to these measures, the Ministry of Home Affairs has launched a scheme – 'Cyber Crime Prevention against Women and Children (CCPWC)'— which includes an online National Cyber Crime Reporting Portal (**www.cybercrime.gov.in**). This portal allows the public to report cases concerning child pornography/child sexual abuse material, rape/assault images or sexually explicit content. The portal also enables individuals to lodge complaints anonymously or through the "Report and Track" option.

UK Government Introduces New Online Safety Bill to Protect Children from Harmful Content

Child protection laws have been evolving in the United Kingdom for several years now, with a focus on keeping children safe from online harm. The Digital Economy Act, 2017 was a landmark legislation in this regard, with provisions that require commercial pornographic websites to verify the age of their users and the establishment of a regulatory framework for online pornography.

The Act also requires Internet service providers to provide parental control filters to their customers to restrict access of inappropriate content by children. Even penalties were levied on online platforms that failed to remove harmful content such as terrorist propaganda, material promoting self-harm or suicide, among others.

Building on this, the UK government has proposed the Online Safety Bill, which aims to improve online safety and reduce harm from online content, especially among children. The Bill proposes to establish a duty of care on online platforms to ensure safety of their users and requires them to take appropriate action against harmful content. The Bill also proposes the creation of a new office— a new independent regulator (the Online Safety Commissioner)— to oversee the implementation of these measures and enforce the duty of care.

The regulator will have the power to issue fines and impose other sanctions, in instances of non-compliance. The Bill covers a wide range of online harms, including illegal content such as terrorist propaganda and child sexual abuse material, as well as harmful but legal content such as cyberbullying, disinformation and online scams. It applies to all online platforms that allow users to share or discover user-generated content, regardless of their size or location.

While the Bill is still subject to scrutiny and debate in the Parliament, it represents a significant step forward towards protecting children from online harms, in the UK. The government aims to strike a balance between protecting children and ensuring that the freedom of expression is not stifled, and the bill is expected to undergo further changes before it becomes law.

The Evolution of Online Child Protection Laws in the US

In recent years, concerns about online child safety have led to the development of various laws aimed at protecting minors from the harmful effects of the Internet. The Children's Online Privacy Protection Act (COPPA), enacted in 2000, was the first federal law aimed at protecting children's online privacy. It requires websites and online services that collect personal information from children, under 13 of age, to obtain verifiable parental consent before doing so. COPPA also requires websites to clearly explain their data collection practices and obtain parental consent before disclosing personal information to third parties.

In 2018, California introduced the California Consumer Privacy Act (CCPA) to further expand privacy protections for minors. This act requires businesses to obtain explicit consent from children aged 13 to 16 years, before collecting or selling their personal information. Businesses are also required to disclose the types of personal information collected, how it is used, and whether it is sold to third parties.

To address evolving challenges, the California Age-Appropriate Design Code Act (CAADCA), effective from 01 July, 2024, will redefine children as individuals under 18 years of age. The CAADCA will also mandate businesses to estimate the age of child users with a reasonable level of certainty. In addition, businesses will be required to design their products and services in a manner that protects the privacy and security of minors.

Recognizing the need for comprehensive online safety measures, the Kids Online Safety Act (KOSA) was introduced, in the United States Congress, in 2022. This Act proposes the establishment of the Office of Kids' Online Safety (OKOS), a federal agency responsible for overseeing online safety for minors. KOSA aims to strengthen regulations regarding social media use by minors and enhance the safety features of these platforms. The Bill suggests setting a minimum age of 13 years for social media use, with parental consent required for users under 16 years. The Bill also mandates annual safety feature audits by social media companies, improvement of accessibility and user-friendliness of safety features and the prompt removal of harmful content within 24 hours of notification.

Protecting Children Online: Australia's Evolving Approach to Online Safety Measures

Australia has a long-standing commitment to protecting children online, as reflected in its history of implementing measures to ensure their safety. The most recent legislation in this regard is the Online Safety Act of 2021, which came into force on 01 January 2022. However, the journey leading to this law has been challenging.

Australia's initial foray into online child safety legislation came with the Broadcasting Services Amendment (Online Services) Act, 1999. This path breaking legislation introduced a co-regulatory framework aimed at shielding children from harmful online content. Under this law, Internet Service Providers (ISPs) were required to offer filtering software to their customers, and a complaints mechanism was established to address online safety concerns.

In 2000, the Australian Government took a significant step by establishing the Australian Communications and Media Authority (ACMA), the regulatory body responsible for overseeing broadcasting and telecommunications, including online safety. Three years later, in 2003, the ACMA introduced the Internet Industry Code of Practice. This code laid down guidelines for ISPs and website operators, fostering a safer online environment through promotion of responsible practices.

Continuing its commitment to online child safety, the Australian government enacted the Enhancing Online Safety for Children Act, 2015. This pivotal law led to the creatin of the office of the eSafety Commissioner, an independent statutory office with a specific focus on promoting online safety for Australians, particularly children. Equipped with substantial powers, the eSafety Commissioner has the authority to investigate and take action against various online safety threats, including cyberbullying and the non-consensual sharing of intimate images.

Recognizing the rapid advancements in online technology and the need for more comprehensive protection for children, the Australian Government passed the Online Safety Act, in 2021. This Act expanded the powers and functions of the eSafety Commissioner and introduced new obligations for Internet platforms and service providers to remove harmful content. Under this law, the eSafety Commissioner possesses the authority to issue takedown notices to social media platforms and search engines, compelling them to remove harmful content targeted at Australian children. Additionally, online platforms are required to implement systems that prevent the spread of harmful content, encompassing issues such as cyberbullying, harassment and misinformation.

INTERVENTIONS BY STATES AND THE PRIVATE SECTOR IN INDIA

Telangana police partners with schools to create cyber safety ambassadors

On the occasion of National Youth Day, the Women Safety Wing of the Telangana Police, in collaboration with the Department of School Education, launched the 'Cyber Ambassadors Platform' (CAP). This initiative aims to empower adolescent students, in schools, by educating them about cybercrimes and promoting preventive measures.

The CAP intends to train 9,424 cyber ambassadors from 2,381 schools across all 33 districts of the state. This includes Government schools, BC Welfare Schools, SC Welfare Schools, ST Welfare Schools, and Minority Welfare Schools. The project involves coordination among various stakeholders, including cyber ambassadors, volunteer mentors, mentor teachers, gender coordinators, and district SHE team officers.

OPPO India partners with CSC Academy to train rural women in cybersecurity

OPPO India, in collaboration with the CSC Academy, has launched the Cyber Sangini programme. The programme is supported by the Ministry of Electronics and Information Technology (MeitY). The programme aims to provide cybersecurity and cyber wellness training to 10,000 women residing in rural and semi-urban areas. The ultimate goal is to empower these women to become certified Cyber Security Ambassadors who can establish local support systems to safeguard vulnerable populations, including women, students, the elderly, and the uneducated, from cyber-attacks.

Upon completing the 45-day course, participants will receive a certificate from National Institute of Electronics and Information Technology (NIELIT), an autonomous scientific society that provides higher and professional education through non-formal sector, that will boost their employment and livelihood prospects within their communities. As Cyber Sanginis, they will be able to charge a nominal fee, for their support, in addressing cybersecurity and cyber wellness issues.

The course covers awareness of existing laws and frameworks designed to protect citizens from cyber incidents such as cyberattacks, cyberbullying, data theft and reputational damage to businesses. This initiative aligns with OPPO's vision of "Technology for Mankind and Kindness for World" and supports MeitYs Stay Safe Online campaign, that strives to promote online safety awareness among citizens.

Meta Launches #DigitalSuraksha Campaign and Take It Down Platform

Meta, formerly known as Facebook, has launched its #DigitalSuraksha campaign aimed at promoting safe Internet use in India, particularly for young people and women. As part of this initiative, the company partnered with the National Centre for Missing & Exploited Children (NCMEC), a non-profit organization that works towards addressing issues related to missing and exploited children. Together, they have introduced the Take It Down platform, which aims to prevent spread of non-consensual intimate images online.

The #DigitalSuraksha campaign was launched on Safer Internet Day 2023 and was followed by the Digital Suraksha Summit that brought together creators, psychologists, educators, civil society organizations (CSOs) and members of parenting communities to discuss online safety issues.

The Take It Down platform, developed in partnership with NCMEC, allows young people to submit a hash of their intimate images instead of the images themselves. These image hashes are then utilized by NCMEC to identify and remove copies of the images from participating applications, thereby preventing their further spread.

Apart from the Take It Down platform, Meta has also introduced several other measures to enhance online safety in India. For instance, it has launched a default setting for teens under 18, on Facebook and Instagram, where they are now automatically assigned private accounts when they sign up on these platforms.

Meta partners with MeitY to promote online safety for G20 Stay Safe Online campaign

Meta, formerly known as Facebook, has announced a partnership with the Ministry of Electronics and Information Technology (MeitY), Government of India, for the G20 Stay Safe Online campaign. This campaign aims to promote online safety and awareness, providing resources in multiple Indian languages through various channels. The resources will cover important themes such as tackling online fraud, reporting harmful content and ensuring personal safety while engaging online. This collaboration between Meta and MeitY will support existing Internet users and benefit new users, in India, aligning with the country's goal of becoming a trillion-dollar digital economy.

In addition to the G20 Stay Safe Online campaign, Meta has also taken steps to address issues related to child safety and online abuse. They have launched an awareness campaign to prevent the sharing of child sexual abuse material, emphasizing the importance of reporting such content. To further promote online safety and wellbeing, Meta has introduced UnGap, a chat show featuring renowned parents and children discussing critical topics including social media use, mental health, and digital wellbeing.

Experts Call for Cybersecurity Education in Schools

As technology continues to get enmeshed in our lives, with each passing day, experts are calling for a greater focus on cybersecurity education, in schools. With cyberattacks increasing in frequency and sophistication, it is essential that young people are equipped with the necessary knowledge and skills that is required, to stay safe online.

According to Microsoft's Global Safety Survey Index 2023, young people are at a high risk of falling victim to cybercrime. The survey highlights that over half of all cyberattacks target small businesses and individuals and the number of attacks is expected to rise, in the future. This alarming trend emphasizes the urgent need for education in the area of cybersecurity, especially among young people.

Experts argue that cybersecurity education should be a part of the school curriculum, so that the students understand the risks, associated with them and are able to stay away at arms length, from which harms, when they are online. This could include topics such as online privacy, password management, safe browsing habits and being able to identify instances of phishing. In addition to protecting themselves, students should also be taught about their role in protecting others online. This includes reporting suspicious activity and not indulge/aid in the spread of false information.

UNHRC Discusses Protecting Children in the Digital Environment

In a meeting held on 13 March 2023, the United Nations Human Rights Council (UNHRC) engaged in an interactive dialogue with the Special Representative of the Secretary-General on Violence against Children. The primary topic of the discussion was the need to protect children in the digital environment.

At the discussion, Ms Najat Maalla M'jid, Special Representative of the Secretary-General on Violence against Children, presented her report on the protection of children in the digital environment, which outlined the growing risks that children face in the online space and stressed on the urgent need for proactive and sustained preventive measures. The report also highlighted the importance of including children in the decision-making processes, as part of the solution.

Protecting Children Online: Risks and Measures

In today's day and age, children are more vulnerable to online threats and risks than ever before. Due to lack of awareness, experience and sound judgment, there is high likelihood that they will fall prey to cyberbullying, online predators, exposure to inappropriate content, identity theft, online radicalization and sexual exploitation.

Cyberbullying, which involves using technology to bully, harass, or intimidate others, is a primary concern for online safety of children. Online predators may exploit the Internet to lure children which may land them in inappropriate or dangerous situations, where thet maybe exploited sexually or they may even be abducted. Additionally, children may come across inappropriate online content, including explicit imagery and pornography. Identity theft is another major concern, as children may lack the necessary knowledge to protect their personal information online.

To ensure online safety of children, parents and guardians can take various measures, such as setting limits on device use, monitoring online activity, implementing parental controls, educating children about online safety, being vigilant against phishing scams and reporting inappropriate or illegal content. In India, several legal provisions, including the Information Technology Act, 2000, Protection of Children from Sexual Offences Act, 2012, Juvenile Justice Act, 2015 and the Indian Penal Code, 1860, are in force to protect children online.

Also it is crucial to educate children about Internet safety and have in place rules and boundaries, for their online activity. Law enforcement agencies and government organizations must address the issue of online child exploitation and work towards stricter implementation of laws and regulations.

While the Internet offers countless opportunities and benefits for children, it is essential for parents, educators and policymakers to be aware of the risks, so that they take necessary steps to ensure children's safety and well-being, more so when then they are online. Protecting children online is of paramount importance and collaborative efforts are necessary to achieve this goal.

INDIA FUTURE
FOUNDATION

Contact Us

☎ +91-1244045954, +91-9312580816

Building no. 2731 EP, Sector 57, Golf
Course Ext. Road, Gurugram,
Haryana, India – 122003

helpline@indiafuturefoundation.com

www.indiafuturefoundation.com