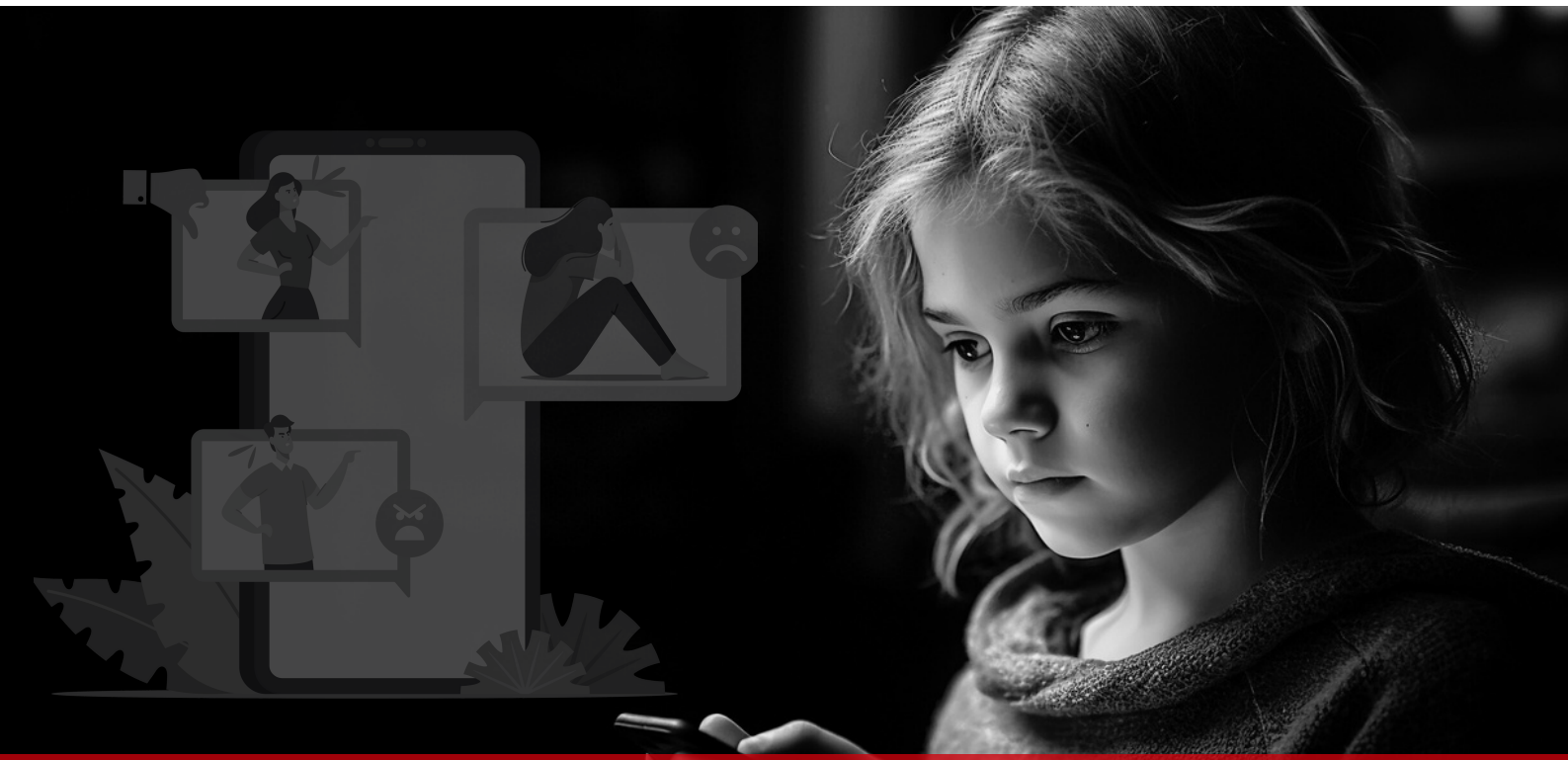
INDIA FUTURE FOUNDATION
Freedom of Expression, Trust and Safety on the Internet

CHILD SAFETY NEWSLETTER



IN THE SPOTLIGHT

In This Newsletter

In the Spotlight.....01

News from around the world.....03

Steps taken by different stakeholders...14

Online Violence Against Children

The interconnected nature of our world, propelled by rapid advancements in information and communication technology, has transformed it into a global village. Social media platforms like Facebook, Messenger, TikTok, Viber, Twitter, Imo, Instagram and WhatsApp have surged in popularity, serving as primary avenues for audiovisual communication. According to the 2023 International Telecommunication Union (ITU) report, a staggering 5.4 billion individuals, accounting for 67% of the world's population, are active Internet users. Notably, 80% of the population aged 15-24 accesses the Internet, with the usage rate in the Asia-Pacific region, as per the study is 66%.

The COVID-19 pandemic has significantly accelerated the proliferation of the Internet, across the globe. The surge in the use of digital platforms for educational purposes has been monumental, benefiting children and young individuals extensively through online learning.

This shift towards online education has extended to teachers and administrators, enabling remote work and education, simplifying daily tasks and enhancing access to information and ideas, seamlessly integrating the Internet into our daily lives.

However, in the midst these advancements, concerns about online violence against children have escalated. The World Health Organization (WHO) reports that one in every three Internet users is a child, with a staggering 800 million children engaged on social media platforms. Unfortunately, this surge in connectivity has seen a disturbing rise in online transgressions, particularly violence against children.

Online abuse against children manifests in various forms, including encouraging them to view sexual acts or pornography, distributing child abuse images, producing explicit videos involving children, cyberbullying and more.

These heinous acts lead to detrimental effects on children's physical, intellectual, psychological and social development, resulting in violence, exploitation, unsafe migration, trafficking and school dropout rates.

A global study conducted by We Protect Global Alliance and Economist Impact revealed alarming statistics, indicating that 54% of the respondents had encountered atleast one form of online sexual harm before they turn 18. In South Asia, 50% of respondents reported experiencing such harms, while in Southeast Asia, the figure stood at 52%. Shockingly, in the Philippines, nearly half a million children were sexually exploited through live online streams in 2022.

Indonesia faces similar challenges, with 2% of Internet-using children aged 12–17 experiencing clear instances of online sexual exploitation and abuse, as reported by a study involving ECPAT International (a global network of civil society organisations that works to end the sexual exploitation of children), Interpol and UNICEF.

In India, underreported online offences against children are attributed to limited awareness of the law and a restricted understanding of abuse or exploitation criteria, with the National Crime Records Bureau (NCRB) acknowledging only reported cases.

Nepal, too, grapples with online child sexual abuse, as highlighted in a study by Voice of Children Nepal and Kindernothielfe Germany, where over 80% of surveyed children encountered online sexual abuses.

The Internet and online platforms, while essential for various facets of life, pose significant dangers, particularly for children and young people who navigate these spaces out of curiosity. Efforts to combat online violence must involve a collective responsibility.

Individuals, including children, families, teachers, Internet service providers and government agencies, bear the responsibility of safeguarding children online. Implementing strong password practices, adjusting privacy settings, cautious engagement with online content and parental monitoring are crucial steps in ensuring online safety.

Collaborative efforts involving informative sessions, enhancing parental skills, effective services from providers and government monitoring and intervention are pivotal in curbing online violence against children. Governments, in partnership with NGOs and private sector entities, should enforce stringent monitoring mechanisms to preserve the Internet's role as a valuable learning resource and safeguard children from online violence.

EU'S CONCERNS OVER CHILD SAFETY ON INSTAGRAM

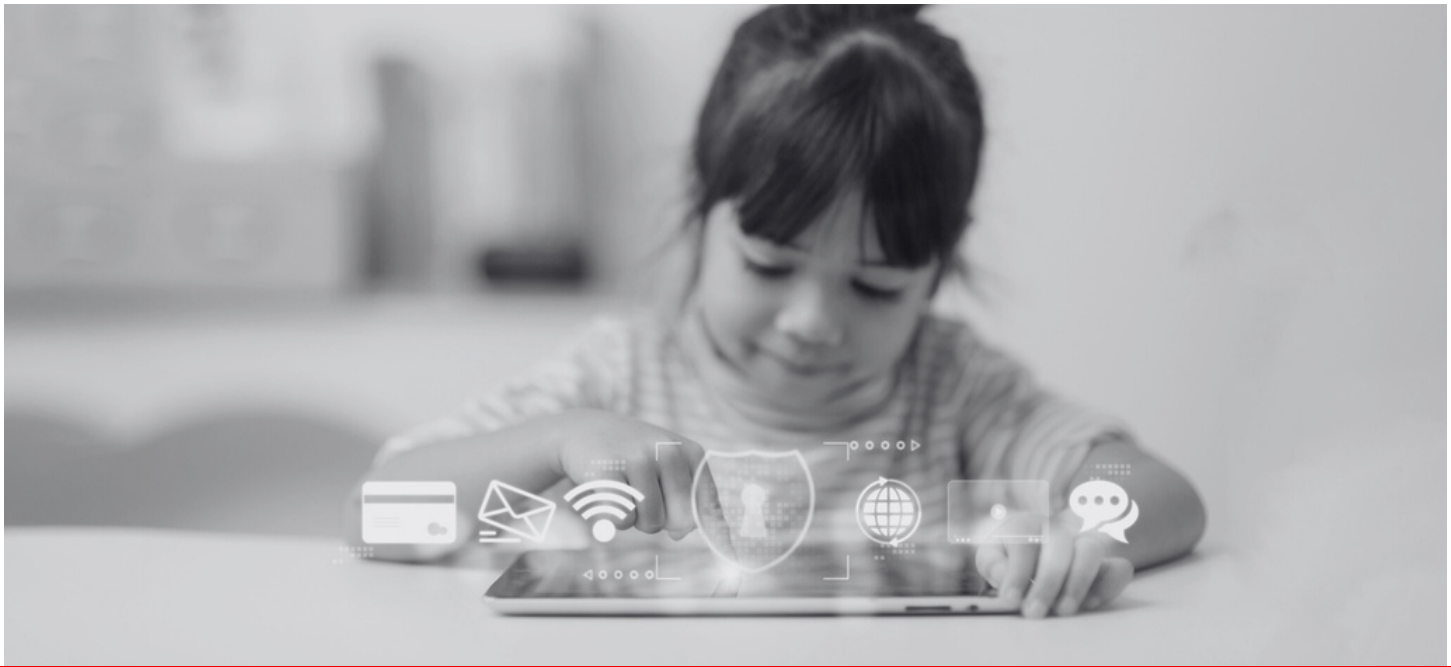
Meta Platforms, the parent company of Instagram, faces intensified scrutiny from the European Union regulators following growing concerns about child safety on the social platform. In response to mounting worries over the sharing of self-generated child sexual abuse material (SG-CSAM) on Instagram, Meta has received yet another formal request for information (RFI) from EU authorities.

The request aligns with the Digital Services Act (DSA), a revised online regulatory framework, applying to larger platforms like Instagram since late August 2023. This act imposes obligations on major tech entities, emphasizing on the need to combat illegal content and prioritize minors' protection. Notably, several early RFIs by the European Commission have revolved around child safety issues, emphasizing the significance of safeguarding young users.

This recent demand for information comes from a report by the Wall Street Journal (WSJ) highlighting Instagram's struggles to address a CSAM issue that was exposed earlier. The report detailed how Instagram's algorithms were linking accounts involved in creating, purchasing and trading underage sex content, prompting concerns about the platform's efficacy in handling such matters.

Despite Meta's establishment of a dedicated child safety task force in response to the WSJ's revelations, another report by the same media outfit suggests little improvement. Tests conducted by the Journal and the Canadian Centre for Child Protection indicate persistent flaws in Meta's systems. Despite efforts to remove problematic content and accounts related to underage sex content, shortcomings remain, with Meta's recommendation systems still occasionally promoting such material.

Meta's lacklustre performance in tackling illegal CSAM/SG-CSAM and addressing associated child safety risks could have severe financial repercussions within the EU. The DSA empowers the Commission to levy fines of up to 6% of a company's global annual turnover for breaching its regulations. Meta was previously fined for violating the bloc's data protection rules for minors, amounting to over half a billion dollars.



In response to these concerns, the European Commission has requested Meta to furnish additional details regarding its measures to mitigate risks linked to protection of minors, specifically addressing the circulation of SG-CSAM on Instagram. The EU has also sought insights into Instagram's recommender system and the amplification of potentially harmful content.

While formal investigation proceedings under the DSA have not been announced yet, the consecutive RFIs indicate the EU's active evaluation, potentially leading to penalties for confirmed breaches.

Meta was given a deadline of 22 December 2023 to provide the Commission the latest tranche of child safety data and Meta reportedly met the deadline. However, the data's specific details and sufficiency haven't been publicly disclosed.

The EU Commission is reviewing the submitted data and assessing its compliance with the DSA's requirements. This review process might take some time.

No formal investigation or penalty has been announced by the EU against Meta at this stage. However, the Commission could initiate an investigation based on their assessment of the provided data. Meta faces further potential compliance hurdles under the DSA. The EU might send additional requests for information or take other actions if they find any discrepancies or insufficient data.

EXPERTS CALL FOR URGENT ACTION IN CHILD SEXUAL OFFENSES

A groundbreaking report from the Childlight – Global Child Safety Institute, operating under the University of Edinburgh's umbrella, emphasizes on the urgent need to address child sexual exploitation and abuse at a global scale, characterizing it as an international public health crisis.

Research conducted by the institute underscores the necessity for updated legislation and policies in response to the evolving landscape of emerging technologies, particularly in relation to child exploitation.

The report, Searchlight 2023, the institute's inaugural annual flagship report, highlighted the substantial role technology continues to play in enabling the exploitation and abuse of children. It emphasizes that the swift evolution of technology introduces new avenues for sexually offending children.

Experts stress on the need for greater accountability and action from online content-sharing platforms to measure and transparently report their efforts in combating online exploitation and abuse.

Childlight's comprehensive review of metrics reported by these content-sharing platforms reveals a lack of transparent reporting of harms. Although 19 company reports were analyzed, the diversity in captured metrics makes it challenging to effectively compare various preventive services' and responsive measures.

Mr Paul Stanfield, Chief Executive Officer of Childlight, voiced concerns over the trends unveiled by the research. The report uncovers distressing data, highlighting the shockingly young age at which many victims experience abuse.

Highlighting the apparent shortfall in protective measures, the report underscores the insufficient efforts made by governments and technology providers to safeguard these vulnerable victims, who cannot often advocate for themselves.

The Childlight report comprises nine new research studies authored by multidisciplinary teams of global experts, delving into the multifaceted nature of exploitation and abuse. These studies aim to provide comprehensive insights into these critical issues.

Childlight, established by the Human Dignity Foundation and situated within the University of Edinburgh, aims to leverage the potential of data to make a tangible difference in safeguarding at-risk children and young people from sexual exploitation and abuse. Their vision is to create a premier, independent data institute that collates and visualizes the prevalence and characteristics of child sexual exploitation and abuse globally, with the primary goal of protecting children.

NEW MEXICO FILES LAWSUIT AGAINST META AND ZUCKERBERG

Mr Raul Torrez, Attorney General of New Mexico, has taken legal action against Meta Platforms, the parent company of social media platforms Facebook and Instagram, along with Mark Zuckerberg, Founder and CEO, Meta. The lawsuit alleges a failure to safeguard children from sexual abuse, online solicitation and human trafficking within social media platforms.

Torrez emphasized that their investigation revealed disturbing evidence indicating that Meta's platforms were not secure for children, providing an environment where predators could exchange child pornography and exploit minors for explicit content.

The attorney general cited instances where Meta allegedly enabled numerous adults to contact and coerce minors into sharing sexually explicit images or participating in pornographic videos.

In response to these allegations, Meta defended its practices, highlighting the use of advanced technology, employing child safety experts and actively reporting content to the National Center for Missing and Exploited Children (NCMEC). Additionally, Meta claims to collaborate with law enforcement and other companies to combat predators, having disabled over 500,000 accounts for violating child sexual exploitation policies in August 2023 alone.

However, Torrez asserted that despite Meta's measures, the company has not implemented sufficient changes to prevent the exploitation of children through its platforms, holding Mark Zuckerberg and Meta executives accountable for the harm caused to young users, through their platform.

This legal action from New Mexico follows similar lawsuits, against Meta Platforms, from other states. Montana's Attorney General recently sued Meta, alleging Instagram's intentional design to be addictive, especially among minors. Additionally, over 40 US states previously sued Meta, accusing the company of contributing to a youth mental health crisis by fostering addictive social media platforms.

The series of lawsuits against social media companies underscores growing concerns about their impact on the mental well-being of children and teenagers. Senators Ed Markey and Bill Cassidy have also accused Meta of intentionally avoiding a children's privacy law and have called for the company to cease this practice.

The legal battles against Meta, TikTok, and YouTube highlight a broader concern regarding the addictive nature of social media platforms, with numerous lawsuits filed on behalf of children and schools citing these concerns.

COMBATTING ONLINE CHILD ABUSE IN 2023

Throughout 2023, the Australian Federal Police (AFP) Central Command, covering South Australia (SA) and the Northern Territory, maintained a crucial emphasis on addressing online child abuse offences. The Joint Anti-Child Exploitation Teams (JACET) in these regions made significant strides, resulting in the arrest of over 100 online child abuse offenders and rescue of more than 77 children from harm, both domestically and internationally. Since its establishment in 2015, the SA JACET has safeguarded more than 345 children.

The JACET teams, comprising of AFP and local police officers, handled an average of 12 online child abuse investigations monthly. Despite variations in the number of investigations between 2022 and 2023, these teams continued their dedicated efforts to combat online child abuse.

In March 2023, the SA JACET achieved a breakthrough, successfully resolving a prolonged online child abuse investigation. This led to the arrest of an individual from Adelaide's southern suburbs after meticulous analysis of images and the application of innovative technology.

Apart from combating online child abuse, the AFP remains committed to various other crime types, including counterterrorism efforts and community engagement. Community Liaison Teams (CLT) organized cultural and sporting events, fostering positive relationships between law enforcement and culturally diverse communities in Adelaide, Mount Gambier and Darwin.

Additionally, airport security remained a critical focus. AFP officers at Adelaide and Darwin Airports responded to numerous incidents, seizing prohibited items and intercepting illicit substances, emphasizing the AFP's dedication to ensuring public safety within airport environments.

FACEBOOK AND MESSENGER ENCRYPTION SPARKS CONCERNS

Meta Platforms recent decision to roll out end-to-end encryption (E2EE) for Facebook messages has triggered apprehension among child safety organizations and prosecutors in the United States of America. While this move by the tech giant aims to enhance user privacy, it has raised significant concerns regarding the potential hindrance it poses to combating child sex trafficking and prosecuting offenders, as voiced by various entities closely involved in child protection.

Under the encryption changes introduced by Meta, the company will no longer have access to the content of messages unless specifically reported by users. This shift significantly impacts content moderation efforts, crucial in identifying and reporting abusive and criminal activities.

The National Center for Missing & Exploited Children (NCMEC) has expressed grave concerns about the impact of encryption on detecting known child sexual abuse material. With Meta previously submitting nearly 95% of the 29 million reports received by NCMEC's CyberTipline in 2022, the potential decrease in reports could substantially hinder efforts to combat child exploitation.

Ali Burns, an assistant US attorney, highlighted the challenges encryption poses to identifying and rescuing exploited children. Access to suspects' private messages often plays a pivotal role in investigations, and encryption could impede law enforcement's ability to gather crucial evidence.

However, civil rights groups emphasize that end-to-end encryption protects personal data and free expression. They argue that creating loopholes in user protections for specific cases could lead to potential misuse by governments and other entities for surveillance purposes.

Meta defended its decision by emphasizing its commitment to user privacy and safety, asserting that they have developed robust safety measures to prevent abuse while maintaining online security. Despite these claims, concerns persist regarding the potential negative impact on efforts to combat child exploitation.

Child safety advocates, including organizations like the Canadian Centre for Child Protection and the Zero Abuse Project, express deep apprehension about the implications of encryption for child safety. They assert that this change could create barriers in collecting evidence and prosecuting criminals who exploit Meta platforms for targeting children.

The introduction of encryption by Meta has sparked a contentious debate between user privacy advocates and those concerned about its potential adverse effects on child safety. The urgency for effective regulation and safeguards to address these concerns remains a pressing issue for both tech companies and advocates of child protection.

META'S ENCRYPTION PLANS RAISE CONCERNS FOR CHILD SAFETY

Meta Platforms, the company behind Facebook and Instagram, has received praise from Australia's e-safety commissioner for its robust reporting of child sexual abuse material. However, concerns have arisen due to looming changes to its Messenger's encryption, prompting worry among child safety advocates and regulators.

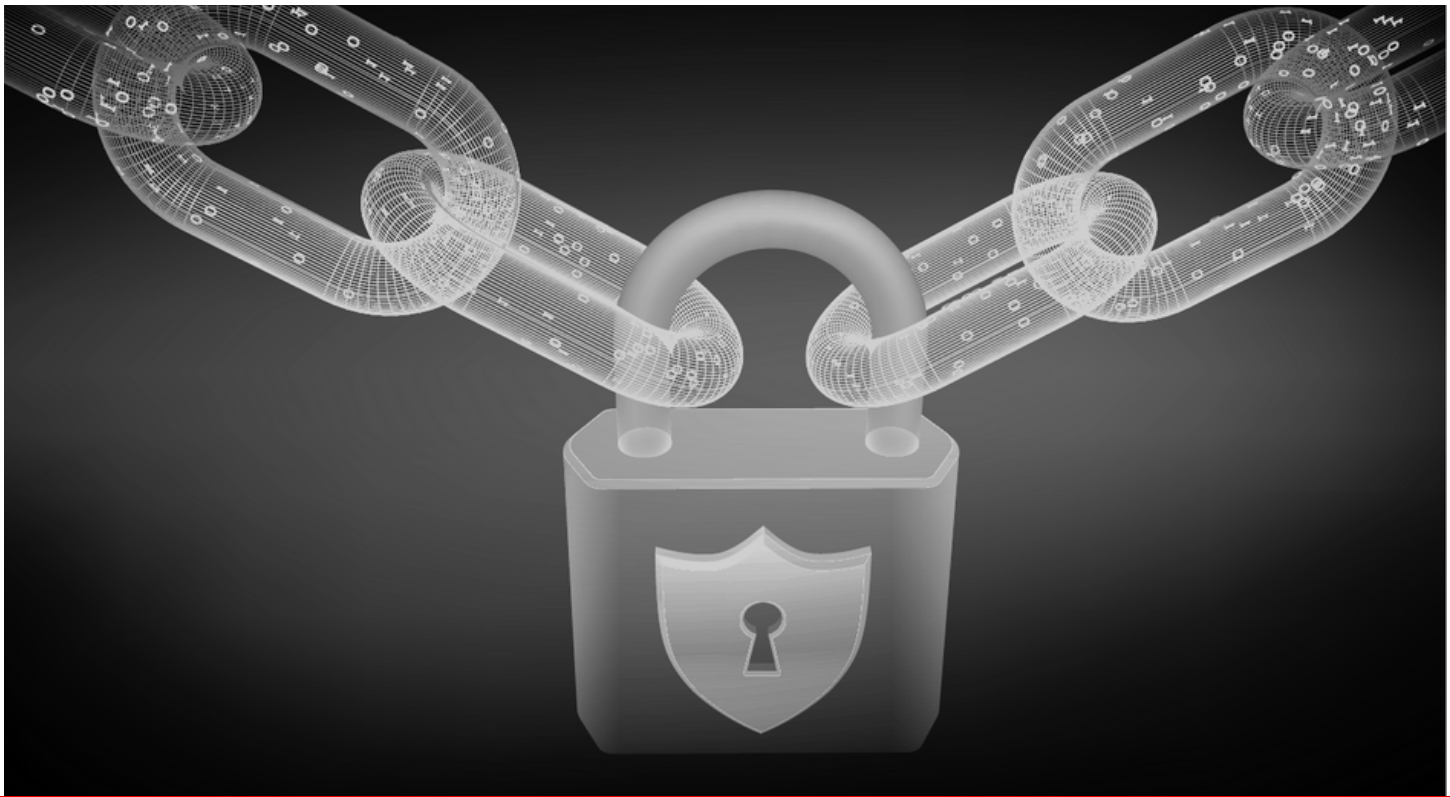
Previously, Meta analyzed Messenger images against databases to report such material. But with end-to-end encryption (E2EE) set to become the default, advocates fear that communications will become obscure, hindering child protection efforts. Despite warnings, Meta is proceeding with this encryption shift, citing the inevitability of such measures.

Meta assures that it has strategies to mitigate harm, aiming to disrupt predatory behaviour by identifying suspicious activity and limiting features for potential threats. The company plans to employ similar technology to detect scams and spam, thereby countering harm on Messenger and Instagram.

The company's approach involves monitoring behavioural signals, restricting messages in question-based on user reports and deploying machine learning (ML) to identify and prevent predators from contacting children. Despite these efforts, critics remain sceptical, anticipating a significant decline in abuse reports following the encryption change.

The readiness of regulators to confront such technological shifts remains uncertain. Past instances, such as the UK's compromise with Apple over iMessage encryption, raises doubts about the ability of the authorities to challenge tech giants. Australia's e-safety commissioner's draft standard accommodates encryption, emphasizing feasible measures without compromising this security protocol.

The clash between technological progress, privacy and child safety intensifies as Meta proceeds with its encryption plans. The efficacy of preventative steps and their measurement remain contentious, fuelling ongoing debates about the balance between user privacy and safeguarding vulnerable individuals online.



KIDS ONLINE SAFETY: NEED TO MAINTAIN A BALANCE

In 2023, federal legislation emerged to safeguard children online, in the United States of America. While these legislation sought to protect young users, they faced backlash as they potentially infringed upon the privacy of children. As a result none of these bills have become law, largely because of the collective effort of digital rights groups and individuals advocating for online rights.

A prominent concern arose when the Kids Online Safety Act (KOSA) was introduced as it was primarily criticized as a censorship bill. KOSA's 'Duty of Care' could compel various online platforms to police content that might cause emotional distress among minors. This legislation, although intended to protect children, raised alarms due to its far-reaching implications on free speech and expression. While KOSA did not progress to a Senate vote, amendments attempting to address its issues failed to resolve fundamental concerns of privacy of young kids.

Another proposed bill, Protecting Kids on Social Media Act, amalgamated controversial elements from existing and proposed laws. This act encompassed age verification, parental consent and data usage limitations, provoking concerns about privacy invasion and unconstitutional mandates.

Although some unconstitutional provisions were removed from the Protecting Kids on Social Media Act, it still faces opposition due to its restrictions on minors' social media access and the creation of a digital ID pilot programme.

One positive outcome of this ongoing debate is the mobilization of young individuals against these bills. Their activation against potential censorship and surveillance signifies a potent force in opposition to such legislative actions. While the intentions behind these bills are commendable, the proposed methods could compromise privacy and censor online speech.

As these discussions persist, the delicate balance between protecting minors and upholding their privacy rights remains a critical focal point. Legislations aiming to mandate age verification and restrict speech, even with noble intentions, often poses constitutional and ethical challenges. The fight against such bills continues, with an expectation of their potential return in altered forms, and the commitment to stand against potential encroachments on online freedom.

TRAINING ON CHILD ABUSE IMAGES RAISES CONCERNS

A recent study has unveiled a troubling discovery. Popular artificial intelligence (AI) image-generators harbour a disturbing amount of child sexual abuse imagery within their foundations. The findings, published by the Stanford Internet Observatory, California shed light on a crucial flaw in these technologies, urging immediate action from companies to rectify this issue.

The report reveals that within the framework of leading AI image-making platforms like LAION, over 3,200 images suspected to be related to child sexual abuse were identified. These distressing images, uncovered by the Stanford group in collaboration with anti-abuse organizations, have significant repercussions.

They not only facilitate the creation of lifelike fake imagery depicting explicit scenarios involving children but also transform innocent, clothed images of real teens into explicit content, raising concerns among educational institutions and law enforcement worldwide.

Previously, experts believed that unchecked AI tools produced abusive imagery by amalgamating adult pornography with harmless images of children. However, this study illustrates a deeper, more unsettling reality within the AI databases.

The immediate response to the report was notable. LAION swiftly announced the temporary removal of its datasets, affirming a zero-tolerance policy for illegal content. While these identified images constitute a fraction of LAION's extensive database of 5.8 billion images, their presence significantly impacts the AI tools' capabilities, potentially perpetuating harm and re-victimizing individuals depicted in these abusive images.

Stability AI, an influential entity involved in LAION's dataset development, acknowledged its role in shaping these datasets. Despite implementing filters to prevent the generation of harmful content, an older version of its model remains accessible and widely used, posing considerable challenges in mitigating the dissemination of explicit imagery.

The report by Stanford emphasizes on the need for immediate and decisive action. It calls upon AI developers who have utilized LAION datasets to remove or cleanse the material. Furthermore, it advocates for the eradication of older versions of harmful AI models from public access.

In response, several tech companies, such as OpenAI and Google, have taken measures to prevent the creation of explicit content involving minors. Nevertheless, there remains a call for stricter regulations and proactive measures across the AI landscape to combat the proliferation of abusive imagery.

The report concludes by questioning the ethical implications of incorporating any photos of children, even innocuous ones, into AI systems without parental consent, citing concerns under the federal Children's Online Privacy Protection Act.

Efforts to curb this alarming trend include proposed solutions such as implementing better content filters, stricter regulations and application of unique digital signatures to AI models to track and remove abusive materials, similar to current practices for images and videos.

The urgency to address this critical issue within AI technology resonates across multiple fronts, emphasizing on the pressing need for comprehensive measures to safeguard against the generation and dissemination of harmful content.

INDIAN GOVT PROPOSES AADHAAR-BASED VERIFICATION

India's Digital Personal Data Protection Act, 2023 proposes a unique two-step verification system to enhance children's online safety, integrating Aadhaar-based consent and parental oversight.

Reportedly, this proposal aims to establish an Aadhaar-based verification system to confirm children's age for accessing online services. Additionally, it seeks parental consent before minors can utilize these platforms. The Act stresses on the necessity for "verifiable parental consent" before granting access to minors.

However, operationalizing this proposal raises concerns about age verification mechanisms for children. The recommendations under consideration involve using parents' DigiLocker app, which relies on their Aadhaar details, or an electronic token system, requiring government authorization.

An anonymous senior government official clarified that this proposed Aadhaar-based authentication wouldn't disclose users' Aadhaar details to Internet platforms. Instead, it would prompt a simple yes/no response from the Aadhaar database, affirming a user's age.

This measure forms one of the 25 rules necessitated for implementing the Act, empowering the government to enact rules deemed essential.

The Digital Personal Data Protection Act, 2023 ratified in August, aims to delineate user rights concerning data use while outlining obligations for entities collecting and processing data. It seeks to render Internet companies, mobile apps and businesses more accountable for citizens' data collection, storage, and processing, reinforcing the Right to Privacy.

This legislative move endeavours to fortify safeguards and ensure greater accountability in managing citizen data, aligning with evolving privacy standards and technological advancements.

CYBERCRIMES AGAINST CHILDREN RISE BY 32% IN A YEAR

In a troubling revelation, the National Crime Records Bureau's 2022 report underlines a distressing surge in cybercrimes against children. The report exposes a worrisome reality where the younger generation is increasingly falling prey to cyber threats, with a notable 32% rise in cases compared to the previous year.

In 2022, the report highlights a stark total of 1,823 cases where children fell victim to cybercrimes, marking a substantial escalation from the previous year's count of 1,376 incidents. According to Mr Sovan Bose, CEO of Child Rights and You (CRY), the concerning aspect is the escalating vulnerability of children in online spaces. Mr Bose expressed that children are no longer safe from online predators. Cybercrimes against children spanned various forms, including cyber pornography, cyberstalking, bullying and other cyber-related offenses.

The COVID-19 pandemic seems to have amplified the risks for children, exposing them to increased online activities for education and entertainment. Mr Bose emphasized on the necessity for robust mechanisms to track offenders and ensure a safer online environment for the younger populace.

The broader analysis of crimes against children paints a distressing picture, showing an overall 8.73% surge in such incidents. The total count stands at 162,449, in 2023, which is in contrast to the previous year's 149,404 cases, as outlined by a comprehensive study by CRY. Further scrutiny of the data unveils a staggering statistic: over 445 crimes were committed against children daily in 2022, averaging more than 18 crimes every hour. The rate of cognizable crimes against children soared to 36.6, in 2022, from 33.6 in 2021, adjusted per every one lakh population of children.

Delving deeper into the decade-long trend, the analysis points to a disturbing pattern. Crimes against children in India skyrocketed by 179% between 2013 and 2022, which is a stark contrast to the overall decrease of 12.3% in the country's total crimes during the same period. This alarming rise underscores the urgent need for enhanced safeguards and stringent measures to protect children in the digital realm while ensuring a robust system to identify and penalize offenders.

The report serves as a wake-up call, urging stakeholders to prioritize the safety and security of children in cyberspace and implement proactive measures to curb these distressing trends.

CHILDFUND SAVE THE CHILDREN AND NETSAFE COME TOGETHER

On 15 December 2023, three non-governmental organisations, ChildFund Australia, Netsafe New Zealand, and Save the Children Australia, joined forces. Save the Children Australia, headquartered at Meta's Sydney Office, will lead this collaborative effort.

In a commendable move, Meta has committed to funding these organisations to provide essential support services and safety education for victims of online abuse, with a particular focus on teenagers and youth. The initiative is set to commence as a pilot programme in Papua New Guinea (PNG), aiming to establish effective reporting pathways for the future.

The core components of this initiative include awareness-raising sessions, establishment of peer safety ambassadors and strategic media campaigns. The industry plans to capitalise on resources from existing partners and the collective expertise of all involved organisations in online safety.

Save the Children Australia emphasised on the importance of online safety, stating, "As children and young people increasingly use social media platforms in PNG and the Pacific, online safety is becoming ever more critical to help ensure their protection from online and real-world harms."

ChildFund Australia echoed similar sentiments, recognising the rapid evolution of the digital landscape in PNG and the Pacific. They emphasised on the urgency for collaboration among the development sector, the tech industry, government regulators and communities to address risks for children in this changing environment proactively.

Netsafe New Zealand, drawing on its longstanding association with Pacific nations, highlighted the need to equip communities with local responses to online harm. In an era where lives are increasingly moving online, they underscored the importance of proactive measures.

Meta, expressing its commitment to responsible digital engagement, acknowledged both the transformative potential and risks associated with the expanding access to digital tools across the Pacific Islands. Meta proudly affirmed its investment in digital literacy initiatives in the region and its role as a founding supporter of this innovative collaboration.

In essence, this partnership not only addresses the immediate challenges of online abuse but also positions itself as a pioneering effort to foster a safer and more responsible digital environment, emphasising the collective responsibility of various stakeholders in safeguarding the well-being of children and youth in the Pacific region.

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