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

CHILD SAFETY NEWSLETTER

In the Spotlight

In This Newsletter

Tech Giants Collaborate to Combat Online Child Abuse

A coalition of tech leaders, including those from Google, Meta Platforms and Discord, unveiled 'Lantern,' a groundbreaking initiative aimed at combating online child sexual exploitation and abuse (OCSEA). Lantern is a pioneering cross-platform programme designed to address this critical issue.

Explaining the urgency of the situation, the coalition highlighted the dangers of online grooming and financial extortion of young individuals. Predators often establish connections on public platforms, disguising themselves as peers or new friends, before coercing victims into private chats to solicit and distribute child sexual abuse material (CSAM) or extort payments by threatening to share intimate images.

Recognizing that these abusive activities span multiple platforms, the coalition emphasized that a comprehensive understanding of the harms faced by victims requires collaborative efforts. Lantern facilitates secure and responsible sharing of signals indicative of policy violations related to child sexual exploitation and abuse among technology companies. This collective sharing of information is crucial

This collective sharing of information is crucial for uncovering threats, enhancing prevention and detection capabilities and streamlining the reporting of criminal offenses to authorities.

The programme's key features include sharing signals such as email addresses, usernames, CSAM hashes, or grooming-related keywords. These signals prompt further investigation, aiding companies in identifying real-time threats to children's safety.

Several notable companies actively participating in the programme's initial phase, include Discord, Google, Mega, Meta Platforms, Quora, Roblox, Snap and Twitch. Addressing concerns about privacy and safety, the coalition emphasized on the establishment of stringent guidelines, ongoing review of policies and mandatory training to ensure responsible data sharing among participating entities.

Meta Platforms highlighted the value of Lantern through a case study involving collaboration with Mega during the programme's pilot phase. Mega shared URLs violating their child safety policies with Lantern, leading Meta's specialized child safety team to investigate and remove over 10,000 breaking Facebook Profiles, Pages, and Instagram accounts.
The collaboration among these tech giants through Lantern aims to create a safer online environment for children by encouraging information sharing, proactive identification of threats and swift action against abusive content.

News from Around the World

RULES FOR BIG TECH TO TACKLE ONLINE CHILD PORNOGRAPHY

Lawmakers in the European Union (EU) have agreed to create new regulations requiring tech giants like Alphabet's Google and Meta Platforms to find and remove child pornography from their platforms. They've clarified that these rules won't interfere with end-to-end encryption.

This rule about child sexual abuse material (CSAM) has been a point of disagreement between people who want more online safety and those concerned about their privacy. The European Commission suggested this rule because the current system, where companies report these things voluntarily, hasn't been enough to protect children.

The proposed rules would make messaging services, app stores and Internet providers report and delete known and new harmful images, videos and grooming cases. They're planning to set up a particular EU Centre on Child Sexual Abuse to gather reports and pass them on to the police.

To avoid spying on everyone, lawmakers made rules for finding and deleting child abuse material stricter. They said authorities can only search for these things if they have a good reason to suspect child sexual abuse.

Companies can pick the technology they use to find these things, but it needs to be checked by an independent group to make sure it works correctly.

Privacy activists praised the decision to keep end-to-end encryption separate from these rules. They think it's an excellent move to stop general spying and only allow checking on specific people with legal permission if there's suspicion of child abuse.

The final details of these rules need to be discussed and agreed upon by EU lawmakers and member states, which might happen in 2024.

This step by the European Union Parliament aims to balance online safety for children while respecting people's privacy on the Internet.

TELEGRAM FACES COMPLAINTS OVER CSAM CIRCULATION

A recent undercover investigation by a Hyderabad-based NGO uncovered distressing findings – Child Sexual Abuse Material (CSAM) is alarmingly circulating on the Telegram messaging app.
Dr Sunitha Krishnan, an Indian social activist and chief functionary and co-founder of Prajwala, a non-governmental organization that rescues, rehabilitates and reintegrates sex-trafficked victims into society, highlighted the grave threat such exploitative content poses to children's safety. She expressed concerns that the circulation of such material could intensify child trafficking for sexual exploitation.

Prajwala complained to Anjani Kumar, DGP, Telengana regarding this issue. Krishnan, raising the issue on Children's Day, emphasized on the vulnerability of children in the age of digital access. Shockingly, some children featured in these videos were as young as three or four. The NGO acquired 38 GB of such content from Telegram groups for a mere INR 600 within a few days.
Krishnan noted that these groups swiftly provided explicit content, each with over 30,000 members. Even when they requested faster delivery, a user responded, stating he attended classes.

Cyberabad Cyber Crime police acknowledged receiving complaints about sharing explicit content on Telegram. They cited a recent complaint in September 2023 regarding the circulation of a rape video for money on the platform.

According to the National Crime Records Bureau (NCRB), 969 cases linked to online transmission of CSAM were reported, in 2023, with a notable increase over the previous years.
Earlier this year, Bangladesh's Criminal Investigation Department (CID) dismantled a Telegram-based child and teen pornography racket, arresting nine individuals involved in blackmailing and selling indecent videos of minors.

Dr Krishnan accused Telegram of enabling exchange of CSAM and explicit content via links, zip files, and private channels without verifying user identities. She pointed out that the app allows anonymity, promoting the sale of such material through private messaging with encrypted options, hindering evidence collection.

Krishnan highlighted that these activities violate various legal provisions under the Protection of Children from Sexual Offences (POCSO) Act, 2012 and the Information Technology (IT) Act, 2000 alongside established guidelines.

TECH CEOS SUMMONES TO US SENATE

In a significant move, the CEOs of major tech companies—Meta Platforms, X, TikTok, Snap and Discord—have been called to testify before the US Senate concerning online child sexual exploitation.

This hearing, scheduled for 31 January 2024, aims to address the failure of these tech giants in safeguarding children on their platforms.

Senators Dick Durbin and Lindsey Graham, Chair and Ranking Member of the Senate Judiciary Committee, USA, jointly announced this hearing, emphasizing the reluctance of Big Tech to take substantial measures to protect children online.

The senators expressed satisfaction that all five companies co-operated after initial resistance, highlighting the CEOs' upcoming testimonies as a pivotal step toward acknowledging the companies' shortcomings in protecting kids, when they are online. They underscored the urgency of action, aligning with the demands of parents and children for safer online spaces.

Notably, the CEOs of X, Discord and Snap will testify following subpoenas issued by the Committee, owing to their prior refusals to engage in discussions. In contrast, the CEOs of Meta Platforms and TikTok agreed voluntarily to testify.

The senators emphasized the tech leaders' previous complaints about not receiving an invitation to hearings. They noted that despite offering them a chance to testify, some companies had declined to make their CEOs available.

The Senate Judiciary Committee will hear testimonies from Mr Mark Zuckerberg, CEO, Meta Platforms; Ms Linda Yaccarino, CEO,X; Mr Shou Zi Chew, CEO, TikTok; Mr Evan Spiegel, CEO, Snap Inc. and Mr Jason Citron, CEO, Discord.

This significant gathering of tech leaders signifies a crucial step towards addressing online child safety concerns. It promises to initiate meaningful actions to ensure a safer digital environment for children.

META FACES CRITICISM OVER ENCRYPTION PLANS

Meta Platforms, the parent company of Facebook, is under fire for its intention to expand end-to-end encryption, with child safety advocates expressing strong opposition to such a move.

Mr Simon Bailey, former chief constable responsible for child protection, based in London, England, United Kingdom, accused Meta Platforms of disregarding social and moral duties by prioritizing profit over children's safety. Similarly, Mr John Carr, representing UK children's charities focused on Internet safety, condemned Meta Platform's move as highly irresponsible.

Mr Graeme Biggar, head of the National Crime Agency, likened Meta's encryption plans to turning a blind eye to child abuse. He urged governmental intervention in defining boundaries between privacy and child safety rather than leaving it to tech companies.

In response, Meta defended its position, assuring robust measures to combat abuse and an expected increase in reports to law enforcement post-encryption implementation.

Bailey criticized big tech, particularly Meta Platforms, for neglecting responsibility in tackling online child sexual abuse. He suggested that Meta's decisions might hinder law enforcement's ability to identify offenders, putting profit before child protection.

Carr echoed concerns about encryption's risk to children, urging Meta to reconsider its approach to prevent endangering child safety and justice.

Ms Rhiannon-Faye McDonald from the Marie Collins Foundation, a victim of online assault, expressed deep disappointment on Meta's encryption plans. She highlighted worries about abuse images being perpetually shared globally, impacting victims and hindering child protection efforts.

This scrutiny highlights a conflict between privacy and child safety online, emphasizing the need for a balanced approach to safeguard privacy and vulnerable individuals, especially children.

STRIKING A BALANCE IN CHILDREN'S ONLINE PRIVACY

In the ever-evolving digital sphere, safeguarding children's online safety is similar to solving a complex puzzle, integrating varied legal frameworks and cultural aspects.

At the IAPP Europe Data Protection Congress 2023, on 15 November, experts highlighted the challenges organizations face to ensure children's digital safety. Discussions encompassed the regulatory landscape, spotlighting stringent measures for children's online protection across significant jurisdictions.

The EU's General Data Protection Regulation (GDPR) sets specific safeguards for children's data, with an age of consent set at 16. Simultaneously, the EU's Digital Markets Act and Digital Services Act impose additional obligations for safeguarding children.

Various U.S. states, such as Arkansas, California, and Utah, have enacted laws protecting children online, complementing the federal Children's Online Privacy Protection Act (COPPA).

Amid these regulations, tech companies like TikTok, Snap, and X (formerly Twitter) grapple with the intricate web of compliance measures. Recently fined by Ireland's Data Protection Commission, TikTok strives to enhance children's protection. Snap and X are aligning functions to address privacy and safety concerns.

However, the encryption debate raises concerns about children's safety. Meta's move toward end-to-end encryption garnered criticism from child safety advocates. The debate around encryption and child safety underscores the need for a balanced approach in prioritizing children's safety over commercial interests.

Integrating artificial intelligence (AI) into children's lives introduces fresh challenges. Policy discussions on AI's impact on children's vulnerability are gaining traction, urging a closer look at children's privacy and protection implications.

Amidst regulatory debates and technological advancements, the paramount focus remains safeguarding children's interests in the digital landscape. Striking a harmonious balance between commercial objectives and children's safety is imperative, emphasizing a child-centric approach in designing digital products and services.

UK CHARITY RAISES ALARMING CONCERNS

The UK Safer Internet Centre (UKSIC) reported incidents of children creating indecent images of other children using AI image generators. This has prompted the charity to call for immediate action to address this disturbing trend before it goes out of hand.

The charity emphasized on the importance of helping children comprehend that producing such images is deemed as child abuse material and illegal under the UK law, irrespective of whether they are real or AI-generated. There is a risk of losing control over such content, potentially leading to online circulation or even blackmail.

This research conducted by RM Technology revealed that nearly one-third of surveyed pupils use AI to access inappropriate online content. This trend suggests a growing knowledge gap between students, who possess an advanced understanding of AI and teachers, making it challenging to ensure online safety, especially of children.

The opinions of teachers diverged on whether it is the responsibility of parents, schools, or governments to educate children about the dangers of such material, indicating the need for a collaborative approach involving schools and parents.

UKSIC stressed on the urgency of addressing this issue to prevent proliferation of harmful content in schools. They highlighted the necessity for interventions, given that new technologies like AI generators are becoming more accessible, potentially leading to increased criminal content creation.

The Marie Collins Foundation emphasized on the potential lifelong damage caused by such images, warning about the risk of material being shared on dedicated abuse sites.

The article highlighted a specific case in Spain where an application using AI created fake nude images of young girls, underscoring the escalating trend of AI-generated content. The application produced realistic photos and despite its potential for misuse, no charges were brought up against those responsible.

The use of "declothing" applications powered by generative AI has become increasingly sophisticated, raising concerns about the difficulty of distinguishing between authentic and AI-generated images. These apps have mass appeal, potentially leading to revenge porn-type activities and causing cultural or religious issues for victims.

The complexity of detecting AI-generated content poses challenges, highlighting the need for immediate action to address these emerging concerns and educate children and educators about the risks associated with AI technology.

UK PASSES ONLINE SAFETY ACT 2023

The Online Safety Act, 2023 has introduced new regulations to safeguard children on the Internet. Under this act, Ofcom, the UK's communications regulator, released initial guidelines restricting direct messaging and preserving children's privacy regarding location data. These measures are intended to counter illegal content, like grooming and child abuse material.
The guidelines emphasize using technology, such as hash matching, to identify and eliminate illegal imagery. Larger platforms are encouraged to implement tools to detect websites hosting such harmful content.

Further rules on safety concerning suicide and self-harm are anticipated and will require parliamentary approval before being enforced, which is expected by next year.

One of the central elements of these guidelines is accountability, requiring tech firms to nominate a responsible person who reports on compliance to senior management.

The initiative is in response to the rise of fraudulent content, mainly driven by advancements in AI, which have been exploited for harmful purposes.

Regulators stress on the necessity of these regulations, highlighting the worsening direction of issues without proper oversight, especially given the exploitation of advanced technologies like AI by malicious actors.

The Technology Secretary emphasized the significance of these initial guidelines in advancing the UK's position as the safest online environment.

Collaboration between regulatory bodies, companies and organizations like the Internet Watch Foundation is crucial for effectively implementing and strengthening child safety measures.

While this legislation marks progress, ongoing efforts are essential to address the escalating risks children face online. Companies play a pivotal role in upholding child safety standards and combating the dissemination of harmful content.

UNDERSTANDING THE ONLINE SAFETY ACT 2023

The Online Safety Act 2023, has stirred a mix of praise and controversy among various sectors. Initially proposed in 2017, the Act aims to make the UK the safest digital space, especially for children, by obligating websites and applications to eliminate illegal content and empowering adults with improved content control.

The comprehensive legislation encompasses a broad spectrum of regulations, expanding from its initial 145 pages in 2021 to nearly double the size presently. It broadly applies to any 'user-to-user service' available in the UK, affecting numerous platforms beyond household names like Facebook, Twitter and TikTok. However, it exempts news organization websites and their comment sections.

One of the Act's key aspects is imposing Duties of Care on user-to-user services to ensure the safety of children and adults, when they are online. This mandate involves conducting risk assessments and the removal of harmful content, encompassing illegal material and newly included categories like self-harm encouragement and cyber-flashing.

The responsibility for enforcing the law rests with Ofcom, the UK's communications regulator, empowering the regulator to block access to non-compliant services within the UK. Failure to comply could lead to hefty fines of 10% of the companies' global turnover and potential imprisonment for executives and employees.

Despite the Act's intentions to protect against harmful content, criticisms persist. The removal of the duty of care for adults regarding 'legal but harmful' content raised concerns of unjustifiable censorship. Critics fear inconsistent standards in determining harmful content and worry about unintended consequences, such as hindering sex education discussions due to content filtering.

Specific provisions of the Act relating to encryption have sparked debates about privacy infringements and potential data vulnerabilities. Messaging applications like WhatsApp, employing end-to-end encryption, face potential challenges due to the Act's power to unlock such encryption, although the government stated its non-utilization until viable.

Opinions on the Act's efficacy vary. Advocates emphasize its necessity in holding tech companies accountable and implementing a regulatory framework to protect children. Conversely, skeptics highlight the reliance on technology alone, advocating for a broader approach involving education and support systems.

While the Online Safety Act 2023 aims to create a safer online environment, debates continue regarding its practicality, potential drawbacks and the need for comprehensive strategies beyond legislative measures to safeguard children and address online risks effectively.

NATIONAL FRAMEWORK FOR CHILDREN'S ONLINE SAFETY

Ahmed Al-Rajhi, Saudi Arabia's Minister of Human Resources and Social Development, unveiled the National Framework for Children's Online Safety during the sixth Saudi Family Forum in Riyadh. The forum, titled "The Saudi Family in Light of Contemporary Changes," witnessed the attendance of the Health Minister Fahad Al-Jalajel and the Media Minister Salman Al-Dossary.

Aligned with the UN Convention on the Rights of the Child, the framework prioritizes safeguarding individuals under 18 years of age. It emphasizes on the critical role of the family in shaping behaviour, preserving cultural values and guiding future aspirations.

Highlighting the Saudi leadership's commitment to family roles in society, Al-Rajhi lauded the integrated efforts with UNICEF to develop the five-year national plan. This plan addresses crucial aspects of children's online safety, including regulations, data protection and support procedures.

The framework's launch signifies collaborative efforts between government entities, the private sector, and stakeholders to fortify children's protection in the digital sphere. The Saudi Family Forum focused on exploring the impact of contemporary changes on families. It engaged experts and officials to offer solutions for family-related challenges posed by the digital revolution.

UNICEF's involvement in the forum included dialogues on protecting children in the cyber world and understanding the digital landscape's implications for children, delivered by experts Professor Amanda Third (PhD), Professorial Research Fellow in the Institute for Culture & Society, and Co-Director of the Young and Resilient Research Centre at Western Sydney University and Al-Tayeb Adam, UNICEF Area Representative for the Gulf.

INTERVENTIONS BY STATES AND PRIVATE SECTOR IN INDIA

KARNATAKA & META PARTNER

Shri Priyank Kharge, IT Minister, Karnataka, , recently announced a plan to collaborate with Meta Platforms, the company behind social media giants Facebook and Instagram, to make the Internet safer, especially for women and kids. He discussed this during the Digital Suraksha Summit, that was held in Bengaluru, on 4 November 2023, where he mentioned how India is quickly becoming digital.

Mr Kharge said that they want to work with Meta to keep women and kids safe online and protect young people from applications like the Chinese loan applications. He mentioned that some illegal applications caused over 60 people in India to lose their lives, and that they have shut a few of them in Bengaluru.

He also talked about a problem with illegal betting applications in smaller towns and villages, which is hard for the government to stop.

Meta Platforms, the patent company of Facebook and Instagram, has been doing things to make the Internet safer, like hosting events and creating tools to help parents control what their kids do online.

They've made special features in their applications, like 'Quiet Mode' on Instagram, which can help people take breaks and tools for parents to see what their kids are doing online. To give an idea, Facebook, has a Safety Centre that has tips and tools in many Indian languages to help parents and teachers keep kids safe online.

This plan between the the government of Karnataka and Meta could mean good things for making the Internet safe for everyone, especially for women, kids and young people.

STEPS TAKEN BY DIFFERENT STAKEHOLDERS

SURAKSHA AUR SAMMAAN' INITIATIVE

In Hyderabad, the Learning Space Foundation's 'Suraksha Aur Sammaan' (Safety and Respect) initiative is making strides in safeguarding children against sexual abuse while educating both youngsters and adults on this critical issue. This five-month project aims to equip children with the skills to identify, avoid and disclose instances of sexual abuse alongside self-defence training.

During the recent Child Safety Week from 14 November to 20 November 2023, the Foundation sensitized over 2,000 students in the Shankarpally Mandal and Rangareddy district government schools. These sessions covered essential topics like recognizing safe and unsafe touches, understanding the POCSO Act, 2012 for children's safety, and crucial lessons on Internet safety.

Smt. Kaumudi Nagaraju, Founder, Learning Space Foundation, and the members of the Foundation and students from Chaitanya Bharathi Institute of Technology, Gandipet, near Financial District, Hyderabad, Telangana, collaborated on this noble cause. They worked closely with local schools, emphasizing the curriculum's importance on personal safety skills.

Kaumudi mentioned that their mission had expanded beyond educating children when they realized the dire need for adult awareness and action. She explained that understanding the responsibility of prevention and protection lay with adults, prompting the Foundation to launch 'Sreyobhilashi,' a programme that focused on educating parents, teachers, police personnel, hostel wardens and NGO workers about child sexual abuse (CSA).

The initiative doesn't stop at educating children and adults. It extends its reach to adolescents, shedding light on laws that impacts them. Most of these youngsters are first-generation learners, often unaware of the laws and the consequences of their actions.

In addition to combating CSA, the Foundation also addresses issues like menstrual hygiene management, mental health awareness and women's safety. They conduct various awareness sessions and support underprivileged communities by providing infrastructure and meeting basic needs.

Through their concerted efforts, the Foundation has reached out to thousands of children and adults across states like Telangana, Andhra Pradesh, Maharashtra, Punjab and Kerala, imparting essential knowledge about CSA, child rights, personal safety, and the legal frameworks protecting children.

This initiative by the Learning Space Foundation aims to empower the vulnerable and build a safer environment by educating and raising awareness among children and adults.

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