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

CHILD SAFETY NEWSLETTER

In the Spotlight

In This Newsletter

India's Digital India Bill to Address Online Safety, Combat Child Sexual Abuse

The Government of India is set to introduce the Digital India Bill, a comprehensive legislation aimed at ensuring strict control over the Internet and tackling emerging cybercrime. Rajeev Chandrasekhar, Minister of State, Ministry of Electronics and and Information Technology (MeitY), Government of India revealed plans for the Bill, which will address various Internet safety concerns, including combating child sexual abuse material, religious incitement material, patent violation material, and misinformation on social media platforms.

The Digital India Bill seeks to hold online platforms accountable for hosting prohibited content and empowers the Government with legal authority to enforce the law. India has witnessed a significant digital transformation, evolving from the most digitally unconnected country in 2014 to becoming the largest connected country with 85 crore people currently connected to the Internet. The number of Internet users is expected to grow to 120 crore by 2025.

The proposed legislation aims to create a safe and open Internet environment while safeguarding digital citizens. With India being the largest connected country globally, the ultimate goal is to make it the most trusted and secure nation in the digital landscape. The Bill will place accountability on online platforms to prioritize user safety and foster trust among users.

News from Around the World

UK Leads 69 States in Joint Call to Action Against Online Child Abuse at the UN

In an unprecedented move at the United Nations, 69 member states, including the United Kingdom and the United States of America, have united to issue a powerful joint call to action against the proliferation of child sexual abuse material (CSAM) on the Internet. The statement emphasizes the urgency for greater efforts to protect children and remove harmful content from online platforms.

The call to action comes after two days of expert discussions hosted by the UN Office on Drugs and Crime (UNODC), in Vienna, which was supported by the British government. During the discussions, the participating countries stressed on the crucial role of the private sector in safeguarding children from sexual exploitation.

Addressing the issue of end-to-end encryption, Corinne Kitsell, Britain's ambassador to the UN, expressed particular concern about companies implementing this technology without robust child safety measures. She argued that such measures could complicate the detection and removal of child sexual abuse materials, amplifying the challenges in tackling online child exploitation.

The concerns surrounding end-to-end encryption have ignited debates surrounding the UK's proposed Online Safety Bill. A provision in the Bill grants the communications regulator Ofcom the authority to compel technology companies to monitor end-to-end encrypted messaging platforms for CSAM using accredited tools. However, as of now, no tool has received accreditation for this purpose.

The proposed use of client-side scanning as a solution to address child safety challenges on social media platforms has been supported by two senior directors at Britain's Government Communications Headquarters (GCHQ). This approach was initially considered less intrusive to end-to-end encryption, as the scanning would occur on one of the endpoints rather than compromising the encryption itself.

However, Apple's recent proposal to include client-side scanning in iOS 15 sparked controversy and was eventually dropped after receiving significant criticism, including concerns raised by 14 distinguished computer scientists who outlined the risks posed by the technology.

In response to the UK's Online Safety Bill, Apple, along with WhatsApp, Signal, and other private sector and civil society organizations, issued a joint statement voicing criticism and urging the British government to amend the legislation to protect end-to-end encryption.

The joint statement issued by the 69 member states emphasizes the urgent need for comprehensive action by governments, Internet service providers, access providers, and other stakeholders to protect children from online sexual exploitation and abuse. It also calls for effective dialogue between various entities and sectors to address this critical issue and ensure the safety and well-being of children online.

Social Media Apps Mandated to Shield Children from Dangerous Stunts

Proposed changes to the online safety Bill will require social media platforms, including TikTok, to protect young users from encountering harmful and dangerous stunts or challenges on their platforms. The updated legislation will explicitly address content that encourages, promotes, or provides instructions for challenges or stunts with a high risk of resulting in serious injury, ensuring that users under the age of 18 are safeguarded from such material.

Platforms like TikTok have faced criticism for hosting content featuring dangerous dares, such as the blackout challenge, which prompted users to choke themselves until unconscious and the milk crate stacking challenge, which involved climbing precarious structures. In response to these concerns, TikTok has already implemented guidelines prohibiting the display or promotion of dangerous activities and challenges.

The revised online safety Bill will further require social media companies to proactively prevent children from accessing high-risk content related to suicides, self-harm and self-injury. Tech firms may be mandated to use age-checking measures to restrict under-18s' exposure to such material.

Additionally, social media platforms will be required to introduce more robust age-checking mechanisms to prevent children from accessing pornography. This measure will align with the Bill's existing requirements for mainstream sites, like Pornhub, to implement highly effective age-checking procedures, potentially including age estimation tools based on selfies.

The proposed amendments will also empower the communications regulator Office of Communications (commonly known as Ofcom), United Kingdom to develop guidance for tech firms on protecting women and girls online. Ofcom will be mandated to consult with the domestic abuse commissioner and victims commissioner to ensure the guidance represents the voices of victims.

The updated legislation will introduce criminal penalties for sharing deepfake intimate images in England and Wales. Moreover, platforms will be mandated to seek explicit consent from adult users regarding their preferences for content related to self-harm, eating disorders, or racist material.

Breaches of the online safety Bill, once enacted, will be subject to substantial fines of up to £18 million or 10% of the global turnover. In severe cases, Ofcom will have the authority to block non-compliant platforms.

Advocates of children's online safety have welcomed the proposed changes, while Lady Kidron, a crossbench peer and children's online safety campaigner, described it as a "good news day for kids."

The government has also affirmed its adoption of changes allowing bereaved families easier access to the social media histories of deceased children.

Nearly One in Ten Parents Haven't Discussed Online Bullying with Their Kids

A recent study, commissioned by Find My Kids (a children's safety platform) headquartered in Delaware, United States of America, has revealed concerning trends regarding parental awareness and actions related to online bullying. The survey of 2,000 parents showed that almost three in ten (28%) children aged five to 18 use social media apps like Instagram and TikTok every day, yet 38% of parents remain oblivious to the associated risks of online bullying on such platforms.

Shockingly, 7% of parents have never spoken to their children about online bullying, despite a quarter of the kids surveyed experiencing bullying, either online or in person. Of those bullied, 70% reported being victimized at least three times, indicating a recurring problem.

While 45% of parents have taken measures to ensure their child's online safety, 22% have not done so, either due to lack of knowledge or due to a perceived lack of concern. Surprisingly, more than half of the parents (53%) feel more concerned about real-life bullying at their child's school than online bullying, despite the significant number of children facing bullying situations.

Among the common effects of bullying on children, 29% reported stopping going to school, and 28% said they stopped seeing their friends. Alarming data shows that 35% of youngsters have hidden their feelings from their parents regarding the bullying they endured. However, 81% of parents believe that their children would inform them if they were victims of bullying.

The study, commissioned by Find My Kids to assess how parents tackle online bullying, also revealed that 48% of parents expressed concerns about their child's online safety. While some parents regularly discuss online bullying with their children, 39% admit these conversations are infrequent.

Despite the prevalent risks of online bullying, only 22% of parents feel confident about recognizing the signs of bullying. Vadikh Giniatulin, CEO of Find My Kids, emphasized the importance of parental awareness and communication with children about online risks. To address this issue, Find My Kids allows parents to monitor the apps their children use and their screen time, facilitating open discussions about potential risks.

Among parents who took action, 48% offered support and actively listened to their children, while 39% restricted or monitored their online activities. Furthermore, 27% involved the school or relevant authorities. However, 21% admitted they would let their child handle their bullying issues, avoiding direct involvement.

The study also revealed that 38% of parents were uncertain about the potential impact of online bullying on their child's safety in real life. The emotional toll on parents is significant, with 16% feeling helpless and 29% experiencing anger due to their child's bullying experiences.

Disturbing Rise of AI-Generated Child Abuse Images Exposed

A new report by The Washington Post sheds light on the alarming proliferation of artificial intelligence (AI)-generated "child sex" images across the web, posing significant challenges for child safety investigators and law enforcement agencies. The rise of AI technology has led to an explosion of lifelike images depicting child sexual exploitation, causing grave concerns among experts in child safety.

The report reveals that forums on the dark web are rife with thousands of AI-generated child-sex images. Even more disturbingly, users are sharing detailed instructions on how to create their own realistic AI images of children involved in sexual acts.

Rebecca Portnoff, the director of data science at Thorn, a nonprofit child-safety group, highlighted the deeply troubling aspect of repurposing children's images, including those of known victims, for this heinous purpose. Thorn has witnessed a steady increase in the prevalence of AI images on the dark web since last fall.

The proliferation of AI-generated child sex images poses serious challenges for investigators and law enforcement agencies. Distinguishing between real and fake images becomes increasingly difficult, undermining efforts to locate victims and combat real abuse. The current central tracking system, designed to block known images of abuse, struggles to detect newly-generated AI images, complicating the identification process.

AI tools can also lead to the re-victimization of individuals whose past child sex abuse photographs are used to train models for generating fake images. This exacerbates the already daunting task faced by law enforcement in identifying vulnerable children in harm's way.

The report also sparks a debate on whether AI-generated images violate federal child-protection laws, especially when depicting children who do not exist. Justice Department officials combating child exploitation argue that such images are still illegal, even if the child depicted is AI-generated. Despite this stance, there has been no prior case in the U.S. where a suspect has been charged specifically for creating deepfake child pornography.

In a recent case in Quebec, Canada, a man was sentenced to three years in prison for using AI to generate images of child pornography, marking the first ruling of its kind in the country. As this disturbing trend continues to grow, authorities and technology companies face an urgent need to confront this new challenge in the fight against child sexual exploitation.

Online Child Sexual Exploitation Reports Increase by 52% in Three Years

A deeply concerning trend has emerged in the realm of online child safety, with reports of online child sexual abuse witnessing a staggering 52% increase over the past three years. Child safety advocates are expressing alarm as the National Centre for Missing and Exploited Children reported receiving a staggering 31.9 million tips about child sexual abuse material last year alone.

The urgency of the situation is further highlighted by the FBI's Jacksonville division, which is actively receiving daily reports of children being sexually exploited online. Recent arrests in Clay County and Camden County have exposed the grim reality of child sex trafficking and the disturbing production and distribution of child sex abuse material.

Data from the CyberTipline has revealed a worrisome trajectory in child sexual exploitation cases. The number of tips about child sexual abuse material has been on a rapid ascent, reaching 21 million three years ago, surging to over 29 million the following year, and peaking at 31.9 million last year.

A particularly alarming aspect of this rise is the increase in financially motivated child sexual exploitation, particularly sextortion of minors. Perpetrators often assume false identities, posing as young females to entice teenage boys into sharing explicit photos. Subsequently, they resort to extortion, threatening to publicly expose the photos unless victims pay a ransom.

Equally disturbing is the revelation that some parents are found to be involved in producing and posting explicit images of their own children online, exacerbating the gravity of the issue. In response, the National Centre for Missing and Exploited Children urges minors to confide in trusted adults and report any instances of sexual misconduct, even if it involves a family member.

Advocates of child safety emphasize on the significance of open conversations with children to ensure their safety and well-being. The fear of reporting abuse often leads to incidents of exploitation remaining unreported until discovered by authorities. Prompt reporting and proactive measures are essential in safeguarding vulnerable children from the growing threat of online sexual exploitation.

Meta Launches Task Force to Address Child Sexual Abuse Material

Meta, the parent company of Facebook, has initiated a task force to investigate and combat the spread and sale of child sexual abuse material on its photo-sharing app, Instagram. This action follows a report from the Stanford Internet Observatory, revealing the presence of large networks of accounts, seemingly operated by minors, openly advertising self-generated child sexual abuse material for sale.

The Stanford report found that buyers and sellers of such material utilized Instagram's direct messaging feature, and the platform's recommendation algorithms effectively amplified the advertisements. According to researchers, Instagram served as a key discovery mechanism for this particular community of buyers and sellers due to the widespread use of hashtags, the relatively long lifespan of seller accounts, and the powerful recommendation algorithm.

The findings shed light on the ongoing struggle of Internet companies to detect and prevent the spread of sexually explicit images that violate their content policies. During the pandemic, incidents of intimate image abuse, commonly known as revenge porn, surged, prompting increased efforts from tech companies, porn sites and civil society organizations to enhance moderation tools. A two-year investigation by The Guardian in April highlighted Facebook and Instagram as significant platforms for the buying and selling of children for sexual exploitation.

Instagram's impact on children and teenagers has drawn scrutiny from civil society groups and regulators, who express concerns about predators on the platform, privacy issues, and the adverse effects of social media on mental health. In September 2021, the company paused its plans to develop a separate version of Instagram specifically designed for children under 13, following public backlash. Later that year, Instagram's head, Adam Mosseri, faced questioning from lawmakers after Meta whistleblower Frances Haugen shared documents revealing the harm Instagram causes to a significant portion of its young users, especially teenage girls.

The Stanford researchers estimate that the seller network consists of 500 to 1,000 accounts at any given time. Their investigation was prompted by a tip from The Wall Street Journal, which initially reported on the findings.

Meta asserts that it has strict policies and technology in place to prevent predators from targeting and interacting with teens on its platforms. The company stated that it had dismantled 27 abusive networks between 2020 and 2022 and disabled over 490,000 accounts in January for violating its child safety policies.

A spokesperson for Meta emphasized the company's commitment to combating child exploitation, stating that they aggressively fight against it both on and off their platforms while supporting law enforcement efforts to apprehend and prosecute criminals involved in such activities.

The report further reveals that some Instagram accounts advertised links to groups on platforms like Telegram and Discord, some of which appeared to be managed by individual sellers.

Nepal Faces Growing Concerns Over Online Child Abuse

Nepal is grappling with the alarming rise of online child abuse cases, as evidenced by the recent reports of sexual exploitation and violence against minors through the Internet. The police cyber bureau has reported 110 cases of online sexual abuse against children in the past 11 months alone, highlighting the urgency of addressing this concerning issue.

Disturbing incidents, such as a woman sexually abusing her nine-year-old sister and sharing explicit content with her boyfriend via Gmail, have shed light on the severity of the problem. Another case involved a 20-year-old man befriending a 13-year-old girl through an online gaming app and subjecting her to sexual abuse and threats of sharing explicit content on social media.

The lack of robust legislation and awareness has made Nepal more vulnerable to children-related cybercrimes. While measures like the Online Child Protection Procedure, 2021, were introduced, their effectiveness has been limited, leaving children exposed to various online risks, including cyberbullying, sextortion and harmful content.

Experts emphasize the need for the government to take proactive action in making the Internet safer for children. They recommend incorporating Internet safety courses into the School curricula, establishing police cyber bureaus in all provinces and building capacities of district police offices to investigate online crimes against children.

Moreover, parents play a crucial role in safeguarding their children's online experiences. Increased awareness among parents about the potential harm of online content and responsible guidance can significantly reduce the risks faced by young internet users.

Addressing the growing concerns over online child abuse requires a collective effort from the government, parents, and relevant stakeholders to protect the vulnerable and ensure a safer digital environment for all children.

Discord Under Scrutiny for Hosting Child Exploitation Content

Discord, a popular chat and community platform, is facing criticism for its role in hosting child exploitation content and for failing to implement adequate safety measures. The platform has been flagged as a hub for child sexual abuse material (CSAM), with users openly advertising and sharing explicit content involving minors.

According to a report from NBC News, Discord serves as a breeding ground for child exploitation, where individuals openly celebrate and encourage the sharing of sexual images and videos involving children. Some groups on Discord actively solicit minors to join adult-oriented communities, promoting the exchange of explicit content. The report also reveals the existence of organized rings involved in the production and distribution of CSAM.

While other platforms, such as Twitter, have taken measures to address such content, Discord has been slow to respond. The company claims that it relies on community members to flag issues and investigate reported behaviour, but critics argue that this passive approach is insufficient.

In response to the mounting concerns, Discord has pledged to work with Thorn, a developer of anti-child-exploitation technology, to develop models capable of detecting grooming behaviour and CSAM. However, experts stress that platforms like Discord need to proactively prioritize safety measures from the outset, rather than addressing them later.

Authorities and organizations dedicated to combating child exploitation have faced difficulties in working with Discord. The company's response time to reports have been slow, communication issues have hindered collaboration and there have been instances of evidence disappearing before any action is taken. Discord's request for payment from law enforcement to preserve records related to child sexual abuse cases has also raised eyebrows.

Despite Discord's stated commitment to child safety, watchdogs and officials argue that more needs to be done. Concerns remain regarding the platform's slow response, hosting of communities involved in CSAM and the need for better cooperation with law enforcement.

Discord acknowledges the need for improvement and plans to implement age-assurance technologies and new models to detect child exploitation content. However, critics emphasize the urgency of immediate action to protect vulnerable individuals, particularly minors, from the risks associated with the platform.

Kerala Tops States in Child Well-Being, Meghalaya Trails

Kerala has emerged as the top-performing state in terms of child well-being, in India, according to the India Child Well-Being Report 2021. The report, jointly published by World Vision India, a not-for-profit organization and Poverty Learning Foundation, a think tank, ranks states based on various factors that impact child well-being, including health, hygiene, protection, and school education. Kerala achieved an overall score of 0.89 out of 1, securing the first rank. Other states that performed well include Uttarakhand, Punjab, Himachal Pradesh and Sikkim, occupying the second to the fifth ranks, respectively. On the other end of the spectrum, was Meghalaya which ranked the lowest with an overall score of 0.

The report calculated the overall score by taking the geometric mean of the domain scores related to health, hygiene, protection and school education. Kerala excelled in the domain of health, along with Mizoram and Uttarakhand. Sikkim, Nagaland, and Uttarakhand topped the list in terms of hygiene. The northeastern states of Arunachal Pradesh, Mizoram and Manipur performed the best in terms of child protection, while Kerala, Punjab and Gujarat were leaders in the area of school education.

The report utilized data from various sources, including the National Family Health Survey 5, National Sample Survey Office 2018, National Crime Records Bureau reports, the Unified District Information System for Education (UDISE) 2019-20 report, and the National Achievement Survey 2017.

This ranking sheds light on the performance of different states in ensuring the well-being of children across multiple dimensions. It serves as a valuable tool for policymakers and stakeholders to identify areas that require improvement and implement targeted interventions to enhance child welfare and development in India.

Paedophiles Exploit AI Technology

In a recent investigation, the British Broadcasting Corporation (BBC) has uncovered a disturbing trend where paedophiles are utilizing Artificial Intelligence (AI) technology to generate and trade in realistic Child Sexual Abuse Material (CSAM). The perpetrators gain access to these images through paid subscriptions to popular content-sharing platforms like Patreon (a membership platform that provides business tools for content creators to run a subscription service).

Government Communications Headquarters (GCHQ), the Government of United Kingdom's (UK) intelligence, security, and cyber agency, acknowledges the exploitation of AI technology by child sexual abuse offenders. They have stated that some perpetrators believe that the future of such material lies in AI-generated content. The abusers employ Stable Diffusion software, designed for art and graphic design purposes, to create lifelike images of child sexual abuse, including heinous acts against infants and toddlers.

The dissemination of these abusive images follows a three-stage process. First, the paedophiles create the images using AI software. They then promote these pictures on platforms like Pixiv, a Japanese social media site primarily used by artists sharing manga and anime. Pixiv, is hosted in Japan where sexualized depictions of children are not illegal, has recently taken steps to address the issue by banning all photo-realistic sexual content involving minors.

The National Society for the Prevention of Cruelty to Children (NSPCC), a prominent children's charity, has called on tech companies to take immediate action and address these dangers. They argue that companies must no longer ignore the exploitation of their products for child sexual abuse and emphasized the need for accountability. The UK government has responded by stating that the forthcoming Online Safety Bill will require companies to proactively combat all forms of online child sexual abuse or face substantial fines.

NCRB Organizes Conference Against Rise of CSAM in India

In a bid to address the surge in child sexual abuse material (CSAM) cases in India, top police officials, union ministries, states, civil society and international organizations and Internet media companies convened in Delhi for a crucial meeting. The issue gained further international attention as the United Kingdom recently prosecuted Mathew Smith, a paedophile involved in a child pornography racket with links to India.

According to the National Crime Records Bureau (NCRB), at least 969 cases related to the online transmission of CSAM were registered, in 2022, but officials warned that this number only scratches the surface of the problem. The figures for 2021 were 805 cases, 842 cases in 2020, and a mere 164 cases in 2019, highlighting the disturbing upward trend.

The conference produced several key recommendations, including replacing the term "child pornography" with "child sexual exploitation and abuse" to better reflect the severity of the issue. Other suggestions included sending regular SMS alerts on the matter to all mobile users through telecom service providers and developing standard operating procedures and checklists for stakeholders such as mobile operators, content providers, app developers, public broadcasters, and app stores. Moreover, the establishment of a centralized "Child Cyber Protection Centre" was proposed to serve as a collaborative hub involving lawmakers, policymakers, tech providers, telecom companies and Internet Service Providers.

Lack of FIR Registrations Hinders Effectiveness of NCRP

Through information obtained under the Right to Information (RTI) Act, 2005, only 0.8% of the 195,409 complaints filed from Maharashtra on the National Cybercrime Reporting Portal (NCRP) between January 2022 and May 2023 resulted in the registration of a First Information Report (FIR). The data further reveals that nationwide, only 2% (42,868) of the total 2,099,618 complaints received during the same period were converted into FIRs.

According to retired police officers from Maharashtra, the insufficient number of inspectors within the cybercrime department is believed to be the primary reason behind this dismal conversion rate. Under the provisions of the IT Act, 2000 only police officers of the rank of inspector and above are authorized to investigate cyber cases. This limitation, experts argue, not only hampers the department's ability to register cases promptly but also undermines public trust in law enforcement agencies.

RTI activist Jeetendra Ghadge, responsible for obtaining this crucial information, expressed concern over the lack of FIR registrations by states, which severely diminishes the effectiveness of the NCRP. While the portal has made it easier for citizens across the country to register complaints, the failure to convert these complaints into FIRs significantly limits the portal's impact in combating cybercrime.

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