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

CHILD SAFETY NEWSLETTER

In the Spotlight

In This Newsletter

HAPPINETZ'S INTERNET SAFETY REVOLUTION

In today's digital age, children's exposure to the Internet is growing at a rapid pace, emphasizing on the critical importance of ensuring a safe and secure online environment. To address this need, the Department of Telecommunications, Government of India, has been actively promoting the installation of Parental Control filters that are designed to monitor, restrict and guide children's Internet usage while blocking inappropriate content.

One of the most concerning consequences of unrestricted Internet access on children is the rise in cases of addiction to online gaming, which can significantly impact a child's mental health, behaviour, and learning. As this problem grows, parents seek practical tools to safeguard their children's online experiences.

While Western markets offer a wide range of parental control filter options, these solutions do not always align with India's distinct parenting styles and values. Indian parents have been searching for a locally tailored solution—Happinetz could be one of them.

Happinetz offers Indian parents a comprehensive parental control filter tailored to meet their requirements. This innovative solution, often called "The Safe Internet for Kids," empowers parents to monitor and effectively guide their children's Internet usage.

Happinetz scans through an extensive database, monitoring over 110 million websites and ensuring that children are only exposed only to content that is appropriate for their consumption. Richa Singh, the co-founder and CEO of Happinetz, started Happinetz recognizing the negative impact of consumption of inappropriate content by young minds.

So what exactly is Happinetz? It is a parental control filter, which effectively blocks over 22 million adult and unsecured websites and applications, thereby ensuring online safety, especially of children. This filter can be integrated with various routers, devices, web browsers and is compatible with multiple platforms.

The way Happinetz functions is that it employs a sophisticated multi-level filter system that categorizes the Internet into 15 categories. Adult and security-related content is automatically blocked, while Safe Search remains active. This multi-level filter acts as a gatekeeper, scrutinizing every child's request for Internet access before allowing or denying it, creating a secure online environment. Additionally, the filter offers curated age-appropriate games through a dedicated "Game for Kids" category, thereby ensuring that children can safely access wholesome entertainment.

The expansive and unregulated nature of the Internet poses numerous challenges, especially regarding safeguarding children when they are online.

News from Around the World

UK URGES META, DELAY ON ENCRYPTION

In a move that has stirred a significant debate, Meta, which employs end-to-end encryption for WhatsApp, has announced its plans to extend this encryption to its Messenger and Instagram's direct messaging services. However, the United Kingdom (UK) has raised serious concerns and urged the tech giant to proceed cautiously.

The call for caution comes after the Online Safety Bill passed on 19 September 2023 by the UK Parliament emphasizes on the need for stringent safety measures to protect children from potential sexual abuse on online platforms. In response to Meta's intentions, Britain's Home Secretary, Suella Braverman expressed concerns, noting that Meta had failed to provide assurances about keeping their platforms safe/free from abusive content.

While advocating for strong encryption to ensure online users' privacy and security, Braverman emphasized that the safety of children must not be compromised. She insisted that Meta implement appropriate safeguards alongside their plans while extending end-to-end encryption to its other applications as mentioned above.

In defence of their decision, to extend end to end encryption to their other platforms beyond WhatsApp, a spokesperson from Meta explained that the company's stance was based on the fact that many Britons already depend on applications that employ encryption to safeguard their privacy from potential threat actors such as hackers, fraudsters, and criminals. The spokesperson, from Meta, emphasized that Meta respected people's desire for privacy of their messages. As a result, they invested five years in developing comprehensive safety measures to prevent, detect and address abuse while ensuring online security and safety. Meta intends to provide an update on the measures they are taking to address these concerns, which may include restricting communication between adults and teenagers who do not have a mutual connection and utilizing technology to identify and take action against malicious behaviour.

Meta also reassured that even as they roll out end-to-end encryption, they are committed to working closely with law enforcement agencies to provide more reports than their peers, underlining their dedication to keeping people safe in the digital realm.

The Online Safety Bill imposes stricter requirements on social media platforms to protect children from harmful content, especially when they are online. However, the introduction of end-to-end encryption has become a contentious issue between technology companies and the government with this new legislation.

Messaging platforms, notably led by WhatsApp, have expressed concerns over a provision, in the bill, that they believe could compel them to undermine end-to-end encryption. In contrast, the government maintains that the bill does not outrightly ban the use of technology but seeks to force companies to combat child abuse by developing technology to scan encrypted messages as a last resort.

The tech industry contends that such scanning and end-to-end encryption are fundamentally incompatible. The ongoing debate between companies and government entities highlights the tension between the need for privacy and the urgency to protect vulnerable users online.

BIG TECH VS. CHILD SAFETY

Childhood trauma, mainly stemming from sexual violence, can leave lasting scars. Mié Kohiyama, from France, a child rights activist and survivor of childhood abuse, shared her personal story and raised concerns about the role of tech giants in tackling child sexual exploitation material (CSAM) online.

Mié's testimony serves as a rallying cry, as she emphasizes that her abuse occurred in an era before the Internet and social media platforms. However, the exponential growth of technology and its misuse for disseminating CSAM has left countless children trapped in an ongoing cycle of re-traumatization.

In 2022, the National Center for Missing & Exploited Children's CyberTipline received over 32 million reports of suspected CSAM worldwide, demonstrating the issue's magnitude. Mié points out that this problem is not confined to the dark web but often involves individuals close to the victims.

Tech companies, which possess the capabilities and resources to develop robust safeguards, have been accused of prioritizing profit over children's safety. Mié argues that while technology can be a powerful force for good, tech creators are responsible for implementing safeguards and checks to protect users, especially children.

The responsibility extends to governments and regulators as well. Mié emphasizes that over 60 per cent of reported CSAM is hosted in the European Union (EU). To address this, the EU is considering a legislation called the EU Regulation to Prevent and Combat Child Sexual Abuse Offline and Online. This legislation would require service providers to report CSAM on their platforms and alert authorities to bring perpetrators to justice.

This legislation provides a unique opportunity to protect millions of children from a lifetime of trauma. As the issue of child sexual violence online gains global political attention, the EU can set an influential precedent by voting to protect children and hold tech companies accountable.

Mié's powerful testimony underscores the situation's urgency and her call for action reverberates as an appeal to prioritize child safety over corporate interests in the digital age. The survivors of child sexual abuse and their allies look to the future, hoping that the EU and tech companies will rise to protect the most vulnerable among us.

CALIFORNIA'S CHILD PROTECTION LAW BLOCKED BY FEDERAL JUDGE

On 18 September 2023, a federal judge issued a preliminary injunction that prevents the state of California from enforcing a law designed to safeguard children's online experiences, citing concerns that the law's commercial speech restrictions may infringe upon the First Amendment of the U.S. Constitution.

The U.S. District Judge Beth Labson Freeman, based in San Jose, California, acknowledged the potential risks children face when using the Internet but found that California's law was too broad in its approach.

The legislation in question, known as the California Age-Appropriate Design Code Act, was passed unanimously by the State Legislature in September of the previous year and was signed by Governor Gavin Newsom. This Act obliges online platforms to evaluate whether their products and services could harm children before making them available. It also requires these platforms to determine the ages of child users and configure privacy settings accordingly or provide high privacy settings for everyone.

It is scheduled to take effect on 1 July of the following year. This law also drew a legal challenge from NetChoice, a trade group representing prominent tech companies such as Amazon, Google, Facebook's Meta Platforms, and TikTok's ByteDance. NetChoice argued that the law would compel private companies to act as content censors on behalf of the state of California or face severe penalties of up to $7,500 per child per violation.

In her 45-page ruling, Judge Freeman acknowledged the state of California's stance that businesses had the discretion to establish their policies. However, she argued that this notion clashed with a platform's First Amendment right to decide, on a case-by-case basis, whether to allow one post while prohibiting a substantially similar one.

Freeman also noted that the enforcement of the said law could cause irreparable harm to NetChoice members and potentially restrict adults' access to information, reducing them to read only what is fit for children.

The California Attorney General's office expressed disappointment on the ruling and indicated that they would respond accordingly. NetChoice, on the other hand, welcomed the decision and looked forward to a permanent strike-down of the law to protect online speech and privacy.

This legal development comes amidst a broader conversation surrounding children's online safety and the balance between protection and free expression. Other courts have similarly challenged laws attempting to regulate how children access online content, underlining the ongoing debate about the digital rights and protections of children and adults.

UK AND US UNITE AGAINST CHILD ABUSE

The United Kingdom and the United States of America have joined forces to combat the proliferation of AI-generated child abuse images. Home Secretary Suella Braverman and US Homeland Security Secretary Alejandro Mayorkas have committed to exploring collaborative action to address the alarming rise of these despicable images, that malicious predators create. They have also called on other nations to join their efforts.

This partnership was announced during the Home Secretary's visit to Washington, where she visited the National Center for Missing and Exploited Children (NCMEC), a US-based child protection organization. The NCMEC plays a crucial role in reporting cases of online child sexual abuse to global law enforcement agencies.

Home Secretary Suella Braverman stated that child sexual abuse is a heinous crime that transcends borders and must be combated globally. She emphasized on the importance of tackling the surge in AI-generated child sexual abuse imagery, which not only incites criminals but also hampers law enforcement's ability to identify real victims online. Braverman commended the NCMEC for its tireless work and called on social media companies to prioritize child safety on their platforms.

The Internet Watch Foundation's investigations have revealed a worrisome increase in AI-generated images depicting child abuse, including infants and toddlers. The rise in such content has raised concerns among law enforcement agencies and charities, who fear it will normalize offending and lead to more children being targeted.

Moreover, these AI-generated images could hinder law enforcement agencies in tracking down and identifying victims of child sexual abuse and apprehending offenders. Some AI technologies even allow offenders to create explicit images from benign content, further complicating efforts to combat this disturbing trend.

This collaborative effort with the US follows the passage of the Online Safety Bill through the UK Parliament. The bill holds tech companies accountable for proactively identifying and removing illegal content, including AI-generated child sexual exploitation and abuse material. Ofcom, UK's communications regulator, can direct companies to use or develop technologies to identify and remove such content.

While AI models hold significant potential for the UK's mission to become a science and tech superpower, they pose as-yet-not-understood public safety and national security risks. The UK aims to engage in open dialogue and collaboration with tech leaders, industry experts and like-minded nations to harness the benefits of AI while protecting society.

SNAPCHAT'S TEEN SAFETY MEASURES

Snapchat has unveiled a series of safety measures to protect its teenage users. The update grants users between ages 13-17 more control over who can connect with them through the application. The changes will allow teenage users to connect only with people they know in real life based on existing friend connections or phone book contacts. The user will receive a pop-up notification if the application detects a suspicious person attempting to contact a teen.

Jack Brody, Head of Product at Snapchat, emphasized that these additional protections ensure teens to connect with people they trust. The application will prevent teenagers from communicating one-on-one with someone who isn't already their friend on Snapchat or is an existing contact on their phone.

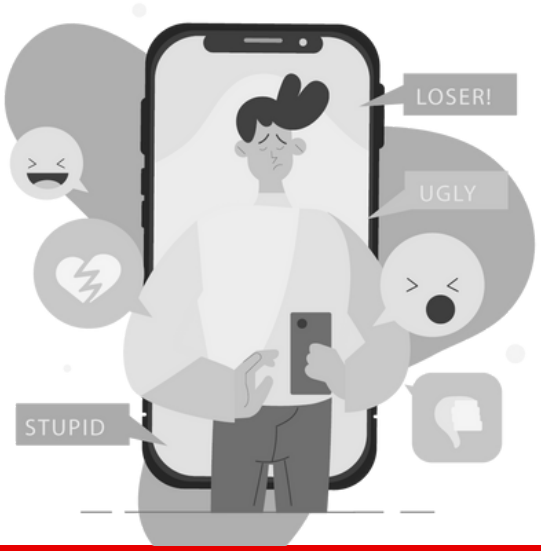
Snapchat has also introduced safeguards to prevent strangers from contacting teens without them having mutual friends. If an unknown person does attempt to contact a teen, the application will allow the user to block the contact confidentially. Default contact settings for teens will be set to "friends and contacts," making it more challenging for strangers to connect with young users.

The platform's Snap Map feature shows users the actual location of their contacts are, and this will be turned off for teen users. If a teenage user chooses to enable it, their location will only be visible to his/her friends and contacts.

Regarding data management, Snapchat noted that while conversations are deleted by default, certain information may be retained for investigation by law enforcement agencies. Brody explained that if authorities require further investigation, they maintain the data for an extended duration.

The platform has also streamlined teen content flow by filtering out age-inappropriate content in the Stories and Spotlight sections. This ensures that suggestive content will not be displayed on the feeds of users aged between 13 and 17.

Snapchat's content labeling process is handled by detection tools that identify accounts spamming users with age-inappropriate content. Accounts that consistently promote such content will face consequences, possibly resulting in a ban, following a strike system.



GOA'S CYBER SAFETY INITIATIVE

To combat the rising threat of online sexual abuse of children in Goa, a state level consultation was organized by the India Child Protection Fund in collaboration with the Goa State Commission for Protection of Child Rights (GSCPCR) in Pilar, on the outskirts of Panaji, on 7 September 2023. The consultation addressed the growing concern of Child Sexual Abuse Material (CSAM) and involved discussions on multi-faceted strategies to tackle this issue effectively.

Prominent officials in attendance, at the consultation, included Peter Floriano Borges, Chairperson of the Goa State Commission for Protection of Child Rights (GSCPCR) and O.P. Singh, former DGP of Uttar Pradesh and CEO of India Child Protection Fund (ICPF). The event emphasized on the need for comprehensive approaches, collective actions involving all stakeholders, increased awareness at all levels and the strict enforcement of the Protection of Children from Sexual Offences (POCSO) Act of 2012.

According to a report by ICPF in April 2020, the demand for child pornography on the public web averaged five million per month in 100 cities across India. Globally, reports of CSAM online have witnessed a 15,000% increase over the past 15 years, according to the National Centre for Missing and Exploited Children (NCMEC).

At the consultation, Peter Floriano, Chairperson of GSCPCR, highlighted on the increased vulnerability of children in the digital era and called for a child-friendly budget to address the issue of CSAM. O.P. Singh, CEO of ICPF, emphasized on the need for efficient utilization of cyberspace, focusing on a time-bound prosecution framework, capacity building for law enforcement agencies and using technology to prevent and prosecute cybercriminals. He also stressed on the importance of raising awareness among the public to ensure the safety of children and create deterrence among perpetrators.

One of the significant challenges discussed during the consultation was decoding CSAM cases from source data received in CD format. According to the data presented by the National Crime Records Bureau (NCRB) for 2021, there has been a more than 400% increase in cybercrimes committed against children in India. In Goa, 43,663 files related to CSAM were downloaded from 30 different URLs in 2021.

The consultation served as an opportunity to generate ideas and discuss the implementation of robust policies and legislative measures to protect children from cybercrimes, including a broader definition of child pornography.

Other dignitaries present at the event included Sampurna Behura, Executive Director of ICPF; Dhananjay Tingal, Executive Director of Bachpan Bachao Andolan; Dr Naveen Chaudhary, Dean of the School of Cyber Security & Digital Forensics and Campus Director of the National Forensic Science University; Akshat Kaushal, Superintendent of Police, Cyber Cell, among others.

SOS CAMPAIGN IN INDIA

A new initiative is taking action to combat the alarming surge in online child abuse cases in India. The SOS Campaign, a joint effort by non-governmental organizations (NGOs) Save Missing Girls and CyberPeace in partnership with PVR NEST, aims to address the less-discussed consequence of the lockdown that has seen an increase in child abuse incidents.

Online platforms have become a hunting ground for child predators, a largely unreported problem, allowing these criminals to evade justice. The SOS Campaign is determined to empower children and their families, encourage communities to create a safe environment for children to speak up and provide solutions and information on prevention and control.

To tackle this issue effectively, SOS seeks to unite all stakeholders. This includes children, parents, schools, psychologists, cyber safety experts, policymakers, law enforcement agencies, and local administrations. The collaborative approach is vital to address the issue comprehensively. A platform called #SOS has been established to facilitate this dialogue.

The SOS Campaign was launched with a unique Public Service Announcement (PSA) film. This film was shown at PVR INOX Cinemas across India, thereby reaching to approximately 20 million parents, families and children to educate them about the nature of cyberspace today.

The PSA introduced the SOS Child Online Safety Desk, an innovative WhatsApp-based tool providing 24/7 assistance to parents and children facing online child abuse. This resource can be reached at 60030 60040.

The SOS Forum, hosted in multiple cities, will hold talk shows with schools to provide students with a safe platform to express their concerns and experiences. The initiative includes SOS Mums, a group of proactive mothers raising awareness about the SOS campaign and the underlying issue. Vigilant parents are encouraged to join the SOS community to advocate for online and offline safe spaces for children.

Leena Kejriwal, the Founder of Missing Link Trust, made a significant statement by pointing out that every 10 minutes in India, a child either goes missing or falls victim to abuse. She emphasized on the urgency of the situation, indicating that it is high time to sound the alarm about this critical issue.

On 15 September 2023, at PVR Juhu, the SOS Community hosted an event featuring discussions on children's online safety with subject matter experts. Following a screening of 'From the Shadows,' an award-winning documentary on child trafficking in India, experts such as Nirali Bhatia, a cyber-psychologist; Ms. Khushbu Jain, a data privacy and technology lawyer; and Dr Nilakshi Jain, a cybersecurity specialist participated.

'From the Shadows,' directed by Miriam Chandy Menacherry, sheds light on the issue of child trafficking in India and the efforts of anti-traffickers like Leena Kejriwal, the co-creator of SOS and founder of SaveMissingGirls. The film follows the journeys of two women working to combat child sex trafficking.

PVR NEST, the corporate social responsibility arm of PVR INOX, one of India's largest cinema exhibitors, aims to raise awareness about online child abuse and child trafficking among its audience. Through its association with the Missing Link Trust and CyberPeace, PVR NEST is helping spread awareness and sensitize people to these social issues.

The surge in online child abuse incidents in India underscores the urgency of initiatives like SOS. In an increasingly digital world, the safety of children must be a top priority, and the collaborative efforts of these organizations aim to create a safer environment for India's children, both online and offline.

STEPS TAKEN BY DIFFERENT STAKEHOLDERS

GLOBAL INITIATIVES FOR CHILD SAFETY

Regulators worldwide have intensified their enforcement of privacy laws designed to safeguard minors online. Video game companies, education platforms, social media networks, smart speaker manufacturers and other digital service providers have faced fines and injunctions for unlawful practices concerning young people's data.

Legislators are also actively scrutinizing online features and content that facilitate excessive information-sharing, bullying, self-harm, eating disorders, substance abuse, addictive behaviours and other potential harms to minors. Consequently, governments are tightening regulations governing online service providers' interactions with children. While many lawmakers agree on the need for more online privacy and safety laws to protect minors, various jurisdictions take different approaches to this shared goal.

For instance, the UK and the state of California have adopted age-appropriate design rules, which outline general principles applicable to almost any business offering online services accessed by minors. These principles require data protection impact assessments, risk-appropriate age assurance measures, tailored settings and digital experiences and strict limitations on privacy-intrusive practices. These rules place the onus on companies to proactively design their services to protect minors' privacy and safety.

On the other hand, some U.S. laws emphasize on the responsibility of parents to act as gatekeepers to their child's internet access. The 1998 U.S. Children's Online Privacy Protection Act (COPPA) requires parental consent for processing certain minors' information. New laws in Arkansas, Louisiana, Texas, and Utah ban social media services from allowing minors to use their features without parental consent. Some laws focus on specific harms related to minors' online activities, like Utah's private right of action against addictive social media platforms or Florida's restrictions on profiling minors and using their data for potential harm or privacy risks.

These privacy and safety laws have arisen in the context of comprehensive data privacy and protection laws. They impose general rules on processing personal data while establishing specific duties related to children's data. Laws like the the EU General Data Protection Regulation and the California Consumer Privacy Act include provisions related to children's data. The age threshold for defining a child varies under these laws, further complicating the landscape.

Companies that offer online services may inadvertently collect minors' data. As such, they should consider the following recommendations:

Conduct Youth Impact Assessments: Undertake individualized impact assessments to identify how personal data is collected, used and disclosed concerning minors and assess the harms they may encounter through the service.

Implement Age Estimation Mechanisms: Ensure compliance with age verification requirements and consider age-gating backed by government ID checks, self-attestations, or biometric scans.

Set "High Privacy" by Default: Default settings for minors should prioritize high privacy, and companies should obtain opt-in consent before minors share their data.

Make Legal Language Clear: Ensure privacy notices and legal terms are clear, concise, and understandable to young users.

Adopt Data Minimization Practices: Collect only the minimum personal data required for core service functionality.

Use AI Responsibly: Avoid using algorithms to make services more addictive to minors and ensure AI-generated content is age-appropriate.

Provide Parental Controls: Encourage or require parental control tools to allow parents to limit their child's data collection and usage.

Implement Robust Security Measures: Protect minors' data from breaches by adopting encryption, secure access controls, security audits, and vulnerability assessments.

Global regulations in this area are rapidly evolving, and adherence to these recommendations can help companies mitigate legal risks and address child safety concerns associated with online services for minors.

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