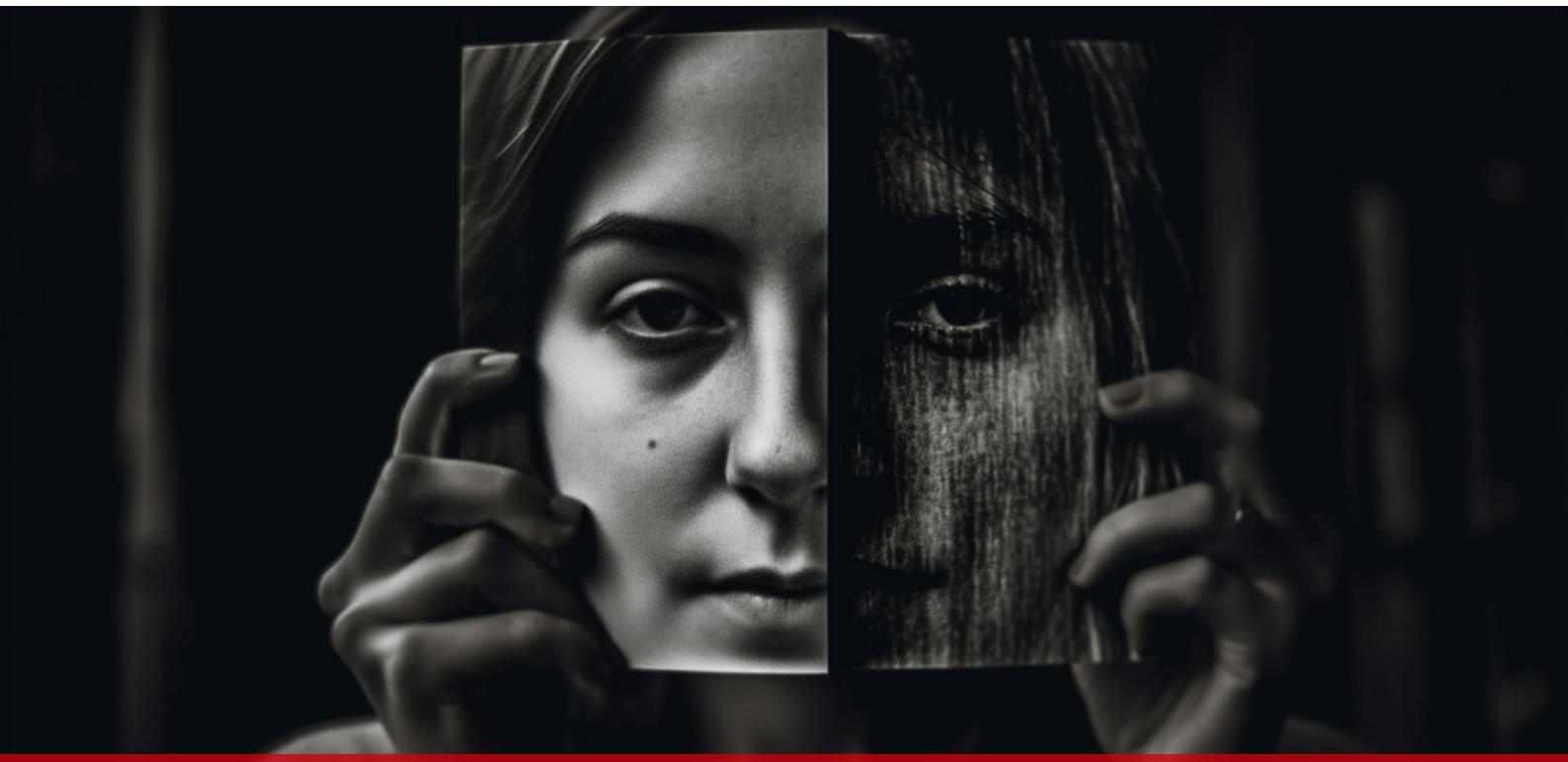
INDIA FUTURE FOUNDATION
Freedom of Expression, Trust and Safety on the Internet

CHILD SAFETY NEWSLETTER



In the Spotlight

In This Newsletter

REMOVE ONLINE CHILD SEXUAL ABUSE MATERIAL

India's Ministry of Electronics and Information Technology (MeitY) has taken a resolute stance against child sexual abuse material (CSAM) on social media platforms and has issued notices to X (formerly Twitter), YouTube and Telegram, demanding the immediate and permanent removal of such content from their platforms, within India. This announcement, made on 6 October 2023, underscores the Government of India's zero-tolerance approach towards harmful and criminal content on the Indian Internet.

To combat the proliferation of CSAM, on social media, MeitY called for the adoption of preventive measures, including implementing content moderation algorithms and reporting systems. These measures aim to prevent the further spread of CSAM, which poses a grave threat to the safety and well-being of children.

The regulatory framework for this action is rooted in the Information Technology Act, 2021, which clearly outlines the obligations of intermediaries.

These intermediaries, regardless of their size, are mandated by Rule 3 (1)(b) of the Act to make reasonable efforts to ensure that their platforms do not host content that is obscene, pornographic, paedophilic, or harmful to children. Furthermore, Rule 4 (4) of the Act stipulates that significant social media intermediaries, are defined as those with over 5 million users in India, must employ technology-based solutions to identify and remove CSAM proactively, from their platforms.

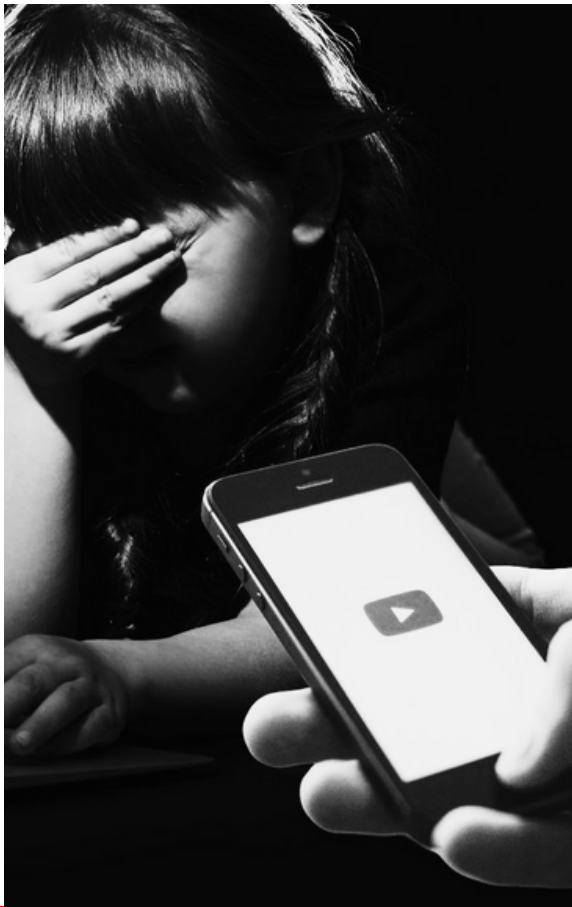
The significance of this development lies in the potential consequences for social media platforms. The Government of India has cautioned that if these platforms fail to take swift action to remove CSAM, they risk losing their safe harbour protection, as outlined in Section 79 of the Act. This means that these platforms could face direct prosecution under relevant laws and regulations, even if they were not responsible for uploading such content, on their platform. Essentially, these companies might lose their immunity from legal responsibility, in India, if they do not adhere to these regulations.

This firm stance taken by the Government of India, since the legislation of the Information Technology Act, 2021, signifies a new era of stricter regulations and potentially sets a precedent for similar actions worldwide. It underscores the growing responsibility that tech companies must be responsible for the content disseminated through their platforms, emphasizing the need for greater accountability in this digital age.

News from Around the World

YOUTUBE DENIES PRESENCE OF CSAM

In response to concerns raised by the Ministry of Electronics and Information Technology (MeitY), YouTube has asserted that it has not detected any child sexual abuse material (CSAM) on its platform. MeitY had issued notices to various social media platforms, including YouTube, instructing them to remove CSAM content, from their platforms. Non-compliance with these directives could lead to the loss of safe harbour protection under Section 79 of the Information Technology Act, 2000.



YouTube, in its formal response to Indian regulators, reaffirmed its dedication to child safety. The company emphasized its substantial efforts to combat child exploitation on its platform. In line with its child safety policy, YouTube disclosed that it had removed more than 94,000 channels and over 2.5 million videos during the second quarter of 2023. According to a YouTube spokesperson, YouTube has a lengthy track record of effectively combating child exploitation on its platform. After conducting several comprehensive investigations,

no instances of Child Sexual Abuse Material (CSAM) were detected on YouTube, nor did they receive any examples or evidence of CSAM on the platform from regulators. The spokesperson emphasized that YouTube strictly prohibits any content that poses a risk to minors and affirmed their ongoing substantial investments in teams and technologies dedicated towards detecting, removing and preventing the dissemination of such content.

Additionally, they expressed a commitment to collaborating with industry partners in the collective effort to halt the spread of child sexual abuse material. YouTube has implemented several measures to protect minors in India. It displays warnings at the top of search results for specific CSAM-related queries, informing users of the illegality of child sexual abuse imagery and providing links to the National Cyber Crime Reporting Portal. The platform enforces an age restrictions, only permitting users over 13 years or those with parental supervision. Accounts of individuals under 13 years without supervision have been terminated. Additionally, YouTube has disabled comments, restricted live features and limited video recommendations that could expose minors to predatory attention.

To further enhance its efforts, YouTube utilizes technology like CSAI Match, an API designed to identify re-uploads of previously identified CSAM material within videos. The company collaborates with smaller partners and NGOs to combat child sexual exploitation on its platform. It encourages user involvement through initiatives like the Priority Flagger, where users and NGOs can report content violating its policies.

MICROSOFT LAUNCHES SINGAPORE XBOX SAFETY TOOLKIT

On 10 October 2023, Microsoft announced the launch of its Xbox Gaming Safety Toolkit for Singapore, aimed at parents and caregivers in the country. This localized toolkit provides an overview of common safety risks and practical advice for ensuring safe gaming experiences for families.

In a first-of-its-kind initiative in the ASEAN region, Microsoft collaborated with local partners, including the Media Literacy Council, Cyberlite Books and SG Her Empowerment (SHE), to design a toolkit tailored to the specific needs of the Singaporean community.

According to Microsoft's Global Online Safety Survey in 2023, 67% of Singaporean parents use at least one form of parental control, compared to 81% of parents worldwide. This reveals the need to raise awareness about parental control options in Singapore.

The Xbox Gaming Safety Toolkit features information on parental and player controls available within the Xbox Family Settings App across various platforms. It emphasizes that parental controls are most effective when used to support existing rules and boundaries established by parents and caregivers.

Microsoft supports safe gaming and ensures player compliance with platform rules. This includes the release of Transparency Reports every six months, outlining the company's efforts to protect players and moderate content. The new toolkit for Singapore complements these efforts by providing clear guidance for parents and caregivers on understanding the gaming ecosystem, common safety risks, and the tools and controls available on Xbox.

In August 2023, Xbox introduced the enforcement strike system, offering players a clearer understanding of how enforcement actions work. This system attaches strikes to each enforcement action based on severity, making it easier for players to comprehend the impact of enforcement actions on their player record.

The Xbox Gaming Safety Toolkit was designed in collaboration with local organizations to ensure its relevance to Singaporean users.

AZURE AI CONTENT SAFETY INTRODUCED

Microsoft has announced the general availability of Azure AI Content Safety within the Azure AI platform. This new system uses advanced language and vision models to help detect harmful content, including hate speech, violence, sexual content, and self-harm-related content. When a potentially dangerous content is seen, the model assigns an estimated severity score, allowing businesses and organizations to tailor the service to block or flag content according to their policies.

Azure AI Content Safety was initially part of the Azure OpenAI Service but is now available as a standalone system. This means customers can use it for AI-generated content from open-source models and other companies' models and user-generated content in their content systems. It expands the utility of the system for a broader range of applications.

As generative AI becomes more mainstream, Microsoft aims to provide businesses with tools to deploy it safely. Microsoft has put nearly 350 employees to work on responsible AI efforts, advocating for accountable AI governance, conducting reliable AI research and creating tools like Azure Machine Learning's Responsible AI Dashboard.

Azure AI Content Safety allows for customizable policies to suit different use cases. For example, a gaming platform may have different content standards than a classroom education platform. The system can also detect potentially objectionable combinations of images and text, like memes.

Microsoft's focus on safety is part of its commitment to building trust in AI, ensuring that consumers can rely on AI technologies to provide safe and secure online experiences.

UK'S ONLINE SAFETY BILL PASSED WITH SUPPORT

The Online Safety Bill in the UK has received the Royal Assent, thereby becoming a law on 26 October 2023. The legislation adopts a zero-tolerance approach to protecting children from online harms while giving adults more choices over what they see online. Many organizations and individuals, including those advocating for children's and women's rights, have supported the new law.

Andrea Simon, Director of the End Violence Against Women Coalition, welcomed the bill for its focus on reducing harm to women and girls online. Lynn Perry MBE, Chief Executive of Barnardo's, praised the duty placed on pornography sites to verify users' age to prevent children from viewing harmful content. William Perrin, a trustee at Carnegie UK, believes that the new regulations will align social media companies with other industries.

X FINED FOR NEGLECTING CHILD SAFETY

In a groundbreaking move, Elon Musk's social media platform, X (formerly Twitter), has incurred a significant fine of 610,500 Australian dollars, signalling a landmark moment in online safety. This substantial penalty marks the first time a digital platform has been held accountable under Australia's Online Safety Act.

The fine stems from concerns related to child abuse content that had increased on the X platform. The incident is a stark reminder of tech giants' responsibility to maintain a safe online environment for their users.

In February, Australia's eSafety Commission called upon several prominent tech companies, including X, TikTok, Google, Discord and Twitch, to provide comprehensive details regarding their measures for detecting and eradicating child sexual abuse content. However, it came to light that X had not satisfactorily responded to these inquiries, leaving certain sections of their response entirely blank.

Under Australian laws introduced in 2021, Internet companies must furnish information about their digital safety practices to the commissioner. Non-compliance with these requirements may result in fines.

Despite earlier statements from Elon Musk emphasizing on the priority of eliminating child exploitation on the platform, X's response to the commissioner's questions raised eyebrows. When questioned about how the service prevented child grooming, they asserted that many young individuals didn't extensively utilize their service. Additionally, the company acknowledged that its existing anti-grooming technology lacked sufficient capability and accuracy for implementation on X. The company also failed to respond to inquiries regarding response times for reports of child abuse, measures to detect child abuse in live streams and the number of staff members actively engaged in content moderation.

The significant fine highlights the importance of stringent enforcement of online safety regulations and places responsibility squarely on the shoulders of tech companies to prioritize child safety in their digital realms.

PARTNERSHIP FOR DIGITAL LITERACY AND CHILD SAFETY

A significant step towards enhancing digital literacy and ensuring online safety for children in Bangladesh has been taken as United Nations International Children's Emergency Fund (UNICEF) Bangladesh collaborates with Grameenphone and Telenor. This partnership aims to support over ten million children in Bangladesh, equipping them with essential digital literacy skills and raising awareness, among them, about safe, ethical, and responsible digital technology use.

The initiative, aptly named "Strengthening Digital Literacy and Secure, Ethical and Responsible Use of Digital Technology for Children in Bangladesh," seeks to address the evolving challenges and opportunities presented by the digital landscape.

The UNICEF representative, Sheldon Yett, highlighted the significance of protecting children in the digital era, underscoring that while the Internet provides vast educational opportunities for children, it's equally crucial to prioritize their digital literacy and online safety. This measure aims to shield them from potentially harmful content and online threats that could adversely affect their well-being.

A significant number of students, encompassing 4.2 million in grades 8 and 9, are set to benefit from this initiative. Additionally, 6 million students from grades 8 to 10 will receive multiple sessions tailored to their age, emphasizing on online safety and digital literacy.

The project extends its reach to include 25,000 teachers and 2 million guardians and parents, aiming to disseminate the importance of online safety and digital literacy throughout the community.

Since 2019, UNICEF Bangladesh, Grameenphone, and Telenor came together under Telenor's global partnership programme, working towards raising awareness about safe Internet practices and mitigating online risks. This programme, till now, has trained over 20 million students, teachers, parents and guardians across Bangladesh.

This shared value partnership signifies the commitment of Grameenphone and Telenor towards empowering and protecting the youth of Bangladesh in the digital realm. UNICEF continues to engage with young people, fostering a sustainable and secure future. This collaborative effort serves as a beacon of hope, ensuring that the digital world remains a safe and enriching space for the children of Bangladesh.

TIPS FOR KIDS' SAFETY ON SOCIAL MEDIA

In today's digital age, the rise of cyberbullying and online threats has become a significant concern, particularly when it comes to the safety of our children. As young individuals increasingly engage with the Internet and various social media platforms, they unwittingly expose themselves to multiple forms of cyberattacks, including cyberbullying and identity theft. These threats encompass a broad spectrum, ranging from online harassment to more severe issues such as identity theft and exploitation.

Cyberbullying, a prevalent form of online harassment, involves sending, posting, or sharing negative, harmful, false, or mean content about someone. It can also include sharing personal or private information about someone, often leading to embarrassment or humiliation.

Given these growing concerns, parents and guardians must proactively educate and safeguard their children about inline risks.

Here are some essential safety tips that can help parents protect their children from the perils of cyberbullying:

Review Social Media Privacy Settings: Parents should diligently review and adjust the privacy settings on their children's social media accounts. It is essential to restrict access to family and known friends. Also, teach your children the importance of maintaining strong and unique password to their acounts.

Monitor Social Media Activity: Keeping a watchful eye on your children's social media activity is crucial. Regularly check their accounts, interactions and posts to ensure that their online experience remains safe and positive.

Avoid Sharing Identifiable Information: Encourage your children not to share easily traceable information on social media, such as their exact location. Limiting personal information exposure reduces the risk of being targeted by cyberbullies.

Beware of Friend Requests: Children should be advised not to accept friend requests from strangers on social media. When faced with online bullying, guide them to log out from the site, save the chat messages or emails as evidence and report the incident to their parents, teachers, or trusted elders. Blocking the sender is also an adequate response.

Think Before You Share: Instill in your children the importance of thoughtful sharing online. They should utilize privacy settings to control the content they post, minimizing their vulnerability to cyberbullying.

Password Security: Emphasize on the significance of never sharing their passwords, even with friends. Passwords are private and should be kept confidential to prevent misuse.

Practice Kindness Online: Encourage your children to be kind and respectful when they are online. Being considerate of others contributes to a safer online environment for everyone.

In the face of a world that getting digitized at a rapid pace, ensuring children's online safety has become a top priority. By following these safety tips and maintaining open communication with your children, parents can empower their kids to navigate the digital landscape responsibly and securely. The support of trusted adults is invaluable in ensuring children's safety and well-being online.

NEW YORK AIMS TO LIMIT SOCIAL MEDIA INFLUENCE ON KIDS

On 13 October 2023, Assembly Bill A8149 for the New York Child Data Protection Act was introduced to the New York State Assembly. State officials have taken a significant step towards protecting the mental well-being of young people by introducing a bill aimed at restricting algorithm-based social media feeds for minors. The proposed legislation, supported by Governor Kathy Hochul and State Attorney General Letitia James, addresses concerns regarding inscrutable algorithms used to engage young users on social media platforms for extended periods, potentially affecting their mental health. Under this bill, minors under 18 in New York would require parental consent to access algorithm-driven feeds on platforms like TikTok, Instagram, Facebook, YouTube and others that use personalized content algorithms. While several states have explored wide-ranging bans on social media apps, New York is among the few targeting algorithms more specifically.

The legislation would focus on platforms such as TikTok and its prominent "For You" feed, which continuously presents short-form videos based on user interests and interactions. However, it would not interfere with a minor's access to chronological feeds featuring posts from accounts they choose to follow. Additionally, the bill would empower parents to set time limits for their children's platform usage, including blocking access to social media apps overnight from midnight to 6 a.m. and pausing notifications during that period.

The proposed legislation in New York, potentially up for consideration as early as the 2024 legislative session in January, may face opposition from tech industry groups. Nevertheless, the bill's sponsors, State Senator Andrew Gounardes and Assemblywoman Nily Rozic, are prepared for the challenge. The strong backing from Governor Hochul, who rarely participates in introducing bills, suggests that it has a good chance of success, especially in a State Capitol controlled by Democrats.

In addition to the bill targeting algorithm-based feeds, a second bill unveiled on the same day aims to safeguard children's privacy. It prohibits websites from collecting, using, sharing, or selling personal data from individuals under 18 for advertising purposes without obtaining consent. Both bills empower the state attorney general to take action against platforms that violate these regulations, marking a significant step in prioritizing the well-being and privacy of young users in the digital age.

CALIFORNIA BANS SOCIAL MEDIA IN CHILD ABUSE

California Governor Gavin Newsom has taken a significant step in protecting the welfare of children online by signing AB 1394 into law on 9 October 2023. This legislation is designed to hold web services accountable for their role in "knowingly facilitating, aiding, or abetting commercial sexual exploitation" of children. The new law, passed by California's legislature in late September, will come into effect on January 1, 2025.

AB 1394 introduces a set of regulations and liabilities aimed at compelling social media services to take decisive action against child sexual abuse material. It imposes penalties on websites that knowingly leave reported abusive content online. More broadly, the legislation defines "aiding or abetting" to encompass actions that "deploy a system, design, feature, or affordance that is a substantial factor in causing minor users to be victims of commercial sexual exploitation." To mitigate their risks, online services can regularly audit their systems.

The bill draws inspiration from whistleblower complaints about Facebook's inadequate response to child abuse on its platform and a 2022 Forbes article that alleged TikTok Live had become a hub for adults to prey on teenage users. By enacting AB 1394, California aims to enhance online safety for minors and create a more robust framework for social media platforms to combat the exploitation of children.

This legislation represents a significant effort to ensure that online platforms take their responsibility to protect minors seriously and act promptly to remove harmful content. California is among the states leading the way in implementing online regulations to safeguard the well-being of its youth in the digital age.

GLOBAL THREAT ASSESSMENT 2023 REVEALS ONLINE ABUSE

The latest Global Threat Assessment Report by WeProtect Global Alliance has uncovered an alarming trend, highlighting an 87% increase in reported cases of child sexual abuse material since 2019. This worrisome surge has resulted in over 32 million reports globally, emphasizing the pressing need for a concerted and multifaceted response to safeguard the world's children from this escalating threat.

Significantly, the report underlines that India remains among the countries with urgent reports of children in imminent danger. The number of such referrals has continued to rise since 2020, indicating a troubling trend in the country.

In addition to the surge in reported cases, the report also reveals a shocking 360% increase in self-generated sexual imagery involving children aged 7-10 years from 2020 to 2022. It further underscores the swift escalation of high-risk grooming situations, with conversations on social gaming platforms turning into potential threats within a mere 19 seconds, with an average grooming time of just 45 minutes.

The report also highlights a significant gap between children's perceptions of online risks and the actual manifestation of online abuse, emphasizing the need for age-appropriate online safety education and accessible reporting mechanisms. Furthermore, there is emerging evidence of a correlation between frequent pornography consumption and access to child sexual abuse material.

Vulnerable minorities and marginalized groups, including those based on sexual orientation, race, ethnicity, or disability, are disproportionately exposed to online sexual harm. The report links global instability, including poverty, inequality, and crises such as the COVID-19 pandemic and climate change, to the rise in child sexual exploitation and abuse.

The collective efforts of various organizations and stakeholders are crucial in addressing this pervasive issue and protecting the world's children from the growing threats they face online. Governments, technology companies and civil society must join forces to prioritize prevention, empower children, establish globally consistent regulations and design technology solutions with user safety as a primary consideration.

The findings, contained in the report, are a stark reminder of the urgency and gravity of the situation, underlining the need for a swift, concerted response to ensure the safety and well-being of children in the digital age.

RISE IN FINANCIAL SEXTORTION TARGETING TEEN BOYS

A Washington Post article (https://www.washingtonpost.com/parenting/2023/10/02/teen-boys-sextortion/) from 2 October 2023, discusses the alarming increase in financial sextortion cases targeting teenagers, particularly young boys. Financial sextortion is a form of online extortion where scammers befriend victims online, entice them to send explicit photos and then demand payment under the threat of exposing these photos to family and friends.

Here are some key points from the article:

Increase in Sextortion Cases: The article highlights that the number of sextortion cases involving teenagers, especially boys, has surged in recent years. Scammers exploit their victims' fears, shame, and embarrassment to manipulate and extort them.

National Center for Missing and Exploited Children (NCMEC): NCMEC has received over 12,500 reports of financial sextortion involving minors by July 2023, a significant increase from the previous year.

Online Safety Experts' Advice: The article provides advice on what to do if a teenager has become a victim of sextortion. This includes immediately ceasing communication with the extortionist, blocking the harasser and reporting the incident to the relevant authorities.

Traumatic Consequences: The consequences of sextortion can be devastating, with several reported cases of teenagers dying by suicide after being blackmailed. The scammers often threaten to expose the victim if they don't comply with their demands.

Global Issue: The problem of sextortion is not just limited to the United States of America; it's a global issue. Authorities have identified West African countries, such as Nigeria and Ivory Coast, as significant sources of these attacks.

Response from Social Media Companies: Social media companies like Meta Platforms (Instagram and Facebook) and Snapchat are taking steps to address sextortion. They have introduced features like high privacy settings for users under 16 years and reporting tools to combat this issue.

Law Enforcement's Involvement: Federal law enforcement agencies are becoming more involved in tackling this problem, recognizing its international scope and the need for cooperation with foreign law enforcement agencies.

The article shared stories of families whose children fell victim to these scams and the emotional toll it takes on them. It emphasizes on the importance of communication and support for teenagers navigating the online world, as well as the need for education and vigilance to protect them from sextortion.

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