**The Special Rapporteur**

**Submission on Existing and Emerging Sexually Exploitative Practices against Children in the Digital Environment by India Child Protection (ICP)**

India Child Protection (ICP) is an organization working to tackle Online Child Sexual Abuse (OCSA) with a focus on promoting both online and digital safety of children. We promote coordinated and strategic efforts, build capacity, leverage grassroots expertise, and apply technology to strengthen child protection nationwide.

**Q1. Please provide information on how technologies are used to facilitate the sexual exploitation and abuse of children.**

The growing internet connectivity & online anonymity are facilitating grooming, recruitment, and sexual exploitation of children with little consequence and impunity. The rise of social media has expanded opportunities for offenders to connect with an increasing number of potential victims, allowing them to interact anonymously, both in India and globally.

Technology is used to sexually exploit children in following ways:

* Predators use social media platforms and chat rooms & Forums to create fake profiles, befriend, manipulate & groom children, gradually gaining their trust before exploiting them and entice them for trafficking. Private images or videos are often shared without consent, often leading to blackmail or further exploitation.
* Platforms such as live video streaming services are used to broadcast abuse / rape of child in real-time.
* Encrypted networks (Including peer-to-peer networks) and the dark web provide anonymity, facilitating the live streaming of child sexual abuse and to share illegal content directly between users while evading detection.
* Online video games are often exploited by offenders to create characters and abuse / sexually exploit other characters (potentially children) inside the game itself.
* Dark Web Marketplaces are used to buy and sell explicit materials, often with complex encryption and Digital currencies and cryptocurrencies offer anonymity for such transactions.
* Abusers can track children’s movements using GPS-enabled devices, often used to arrange meetings.
* AI is used to create realistic but fake images and videos of children (AI-Generated Child Sexual Abuse Material or CSAM), often for the purpose of blackmail or distribution
* VPNs and Proxies are used to hide the physical location of users, complicating law enforcement efforts to trace them.

**Q2. What practical recommendations would you propose for States, the technology industry and online service providers to prevent the sexual exploitation and abuse of children in the digital environment?**

To understand and address the problem of OCSA, ICP has conducted research with technological partners and organizations. In April 2020, ICP released a report on the demand for child pornography and pilot deterrence using AI. Earlier, in October 2019, ICP initiated a study to understand and deter the landscape of CSAM in India. This research is increasingly relevant due to technological advancements driving demand for CSAM and online abuses like grooming and sexual coercion. In 2022, ICP, in collaboration with a partner organization, published "Entangled in the Web: Cybercrimes against Children in India," revealing the impact, extent and measures taken by the Indian Government for tackling CSAM. The Government of India has made significant strides in strictly addressing child pornography through the Protection of Children from Sexual Offences (POCSO) Act, 2012 and the Information Technology (IT) Act, 2000. However, as it is an evolving crime and borderless in nature, it needs comprehensive legislative framework with international convergence.

The studies provide insights and recommendations for stakeholders involved in prevention, prosecution, regulation and rehabilitation of victims and creation of a safe digital environment for children in India.

Recommendations for the States:

* The States must establish a legally binding international convention to facilitate cross-border investigations, sign an international treaty, formulate an international task force (akin to coalitions like G20 and NATO), implement specialized investigation protocols with strict timelines and automatic escalation procedures for unresolved cases.
* The States must standardize and align the international norms, judicial framework and Indian legislations as the disparity and disconnect between them poses a challenge in prosecution of cases received from International Agencies.
* The term ‘Cybercrime’ is used extensively but lacks a legal definition and various terms are used to describe OCSA, including 'pornography', 'CSAM', etc. Standardizing terminology internationally is crucial for comprehensive legal coverage.
* OCSA is a continuous, organized economic offence with far reaching ramifications for economic gain and association with trafficking syndicate, therefore needs to be treated accordingly.
* Nations should develop their own robust institutions for tracking CSAM, reducing dependency on external bodies and enhancing the efficiency of interventions.
* Legislation must be strengthened to address emerging threats, including deep fakes & use of anonymizing technologies, to mandate reporting for ISPs and intermediaries, and to track and regulate financial transactions linked to OCSA.
* Implementing policies to place users of OCSA on sex offender’s registries and ensuring they are barred from jobs involving children will enhance preventive measures.
* CSAM offenders in Sex offender’s Registry to be shared with the Intermediaries, Tech Companies and Online / Digital platforms to monitor and regulate their online activity.
* Sufficient resources must be allocated to law enforcement agencies, including specialized cyber and forensic units, and dedicated budgets should support research, victim rehabilitation, and mental health services.

Recommendations for the Technology Industry:

* Technology Industry must incorporate robust child protection features, including age verification, parental controls, regular risk assessments and mandatory tools for detecting, monitoring, and reporting harmful activities.
* Advanced AI and machine learning tools are essential for detecting explicit content, assigning hash values to explicit content, identifying grooming behavior, flagging and take down of CSAM Content.
* Developing preloaded mobile/system monitoring applications and victim identification systems, along with publishing regular transparency reports on efforts to combat OCSA, are vital measures for enhancing child safety in the digital age.

Recommendations for Online Service Providers:

* Online Service Providers must implement strict guidelines to regulate, monitor, blocking CSAM content and report live streaming of OCSA content to combat Web Cam Child Sex Tourism to Law Enforcement Agencies.
* Intermediaries need Standard Operating Procedures (SOP) and a Code of Conduct for regulation, information sharing with authorities, and compliance with legal frameworks to promote safe online environments.
* Robust age verification mechanisms must be developed to hold perpetrators accountable.
* Investment in joint Research and Development projects is crucial for creating innovative technologies to detect and prevent OCSA.
* Internet Service Providers (ISPs) should be required to publish annual reports detailing their progress in combating abusive content and include a specific compliance report on tackling child pornography for governmental review.

**Q3. What are the remaining gaps that limit the effective implementation and application of existing laws, policies and guidelines to prevent, detect, report and protect children from sexual exploitation and sexual abuse online?**

ICP collaborates with law enforcement and government departments in various states in India to build capacity of officers and support victims, enhancing prosecution of OCSA Cases. The current Indian legislature while addressing the issue of child pornography, empowers law enforcement to act against perpetrators. However, victims and offenders often reside in different jurisdictions, and the 'borderless' nature of these crimes, along with financial linkages, poses significant challenges for tracking and prosecution efforts. Absence of a comprehensive or standardized legislation, definition and alignment with international legislative framework, lack of cross border treaty and international cooperation & coordination creates gaps in implementation and application of existing laws, policies and guidelines.

Law enforcement agencies also face significant resource constraints, lack specialized cyber units, forensic labs, and the necessary training and technology to combat CSAM effectively. As OCSA is not a traditional crime and a digital crime, the investigators and prosecuting agencies lack the knowledge on the evolving method of investigation. The lack of legislation and technology to counter the widespread use of encryption and anonymity tools by perpetrators exacerbates these issues, making detection and monitoring difficult. Additionally, there are deficiencies in age verification mechanisms and victim identification systems, leaving children vulnerable to exploitation. A lack of awareness and education among parents, educators, and children about online risks and safe practices, coupled with the social stigmatization of victims, deters reporting and seeking help.

**Q4. What are the challenges that exist in the use of these digital technologies, products or services, that inhibit the work of law enforcement across jurisdictions in their work to investigate, detect, remove child sexual abuse materials online and prosecute these crimes?**

ICP has been supporting various State Cyber Cells across India by extending expertise and knowledge of digital technologies, products or services and has access to technological tools for the identification and forensic investigation of CSAM cases. It is observed that there are number of challenges that inhibit the work of law enforcement across jurisdictions. The data received by Indian Government from international agencies like Interpol and CyberTipline are huge in volume which creates difficulties in identifying and extracting relevant information in a time-bound manner, and due to discrepancy in international norms, judicial framework and Indian Law poses challenge in prosecution of such cases leading to huge pendency. End-to-end encryption, while protecting user privacy, complicates law enforcement's ability to intercept and access CSAM-related communications. Anonymity networks like the dark web, Tor, and VPNs provide perpetrators with enhanced anonymity, make it difficult to monitor and shut down illegal operations. Cryptocurrencies add another layer of anonymity, complicating the tracking of payments for illegal activities.

Police struggle with limited access to advanced technology, cross border cooperation and training, contribute to high pendency rates of cases. Emerging technologies like AI-generated deep fakes require constant adaptation of law enforcement tactics. Additionally, the lack of victim identification systems and cooperation among intermediaries delays investigations. The absence of standardized mechanisms and procedures complicates the investigation of digital crimes. Data access and privacy laws, bureaucratic hurdles for cross-border cooperation, and platform shifts by perpetrators to evade detection also impede efforts. Perpetrators often move to new or less regulated platforms to evade detection, requiring law enforcement to continuously monitor a broad range of services. Lack of comprehensive, coordinated efforts involving updated legal frameworks, resource allocation, advanced technological tools, and robust international cooperation are road blocks for law enforcement agencies to effectively combat CSAM.

**Q5. What technical and regulatory measures can be put in place by States, the technology industry and online service providers (legislative, regulatory, administrative, institutional and others) towards mitigating human rights risks associated of online child sexual exploitation and abuse, and ensuring the minimum harmonization across legal jurisdictions?**

Technical Measures

* Develop and deploy advanced AI and machine learning algorithms to proactively identify and remove illegal content while respecting user privacy rights.
* Develop encryption standards that prioritize user privacy while allowing for lawful access by authorized authorities under specific circumstances.
* Invest in data analytics tools and enhance data-sharing protocols and platforms among law enforcement agencies, technology companies, and relevant stakeholders to facilitate collaborative investigations.
* Implement age verification mechanisms to restrict access to age- inappropriate content and services, reducing the risk of children encountering harmful material.
* Provide robust parental control features that empower caregivers to monitor and manage their children's online activities effectively.

Regulatory Measures

* Establish international conventions and treaties to harmonize legal frameworks for combating OCSA across jurisdictions.
* Develop model laws and regulations that set minimum standards for online safety, including content moderation, data protection, and law enforcement cooperation.
* Implement penalties for non-compliance with reporting obligations and child protection standards, ensuring accountability of online platforms.
* Require transparency reports from technology companies detailing their efforts to combat OCSA, including data on content removals, user reports, and law enforcement referrals.
* Establish liaison offices / joint task forces / regulatory body dedicated to coordinating efforts between law enforcement agencies across different jurisdictions, and for effective monitoring and regulation of intermediaries, online service providers, etc.
* To establish a real-time tracking, reporting and monitoring system (dashboard) at National level for taking time-bound action against the defaulters / offenders. Proactive mechanism to be in place to alert the international agencies in case of cross-border defaulters.

**Q.6 Are there any other practical examples of internal monitoring, complaint and reporting processes; establishment of regulatory bodies and interventions; remedial pathways; robust safeguarding procedures; children’s rights’ due diligence and risk assessments; and technical standard-setting processes to ensure safety and inclusivity by design?**

Yes, in India, there are initiatives for internal monitoring, complaint and reporting processes, include the following:

* National Helpline Number: Setting up and running of a national helpline number for reporting the incidents of OCSA.
* Ministry of Home Affairs of India has prepared a list of certain keywords and URL sites, which are banned from usage and social media to enable a mechanism to show warning on searching the listed keywords and blocked URLs.

Few examples of technological companies undertaking the monitoring and reporting processes include:

* Facebook’s Community Operations: Facebook employs AI tools to monitor and identify potential OCSA content, supplemented by a team of human moderators who review flagged content.
* Google’s SafeSearch: Automatically filters out explicit content from search results, ensuring that children are less likely to encounter harmful material.
* YouTube’s Reporting Tool: Allows users to report inappropriate videos, which are then reviewed by YouTube’s trust and safety team.
* Twitter’s Report Abuse: Provides a streamlined process for users to report abusive behavior or harmful content, with a dedicated team handling these reports.
* Apple’s iOS Parental Controls: Integrate privacy and safety features into the design of the operating system, allowing parents to control their children’s app usage and content access.
* WhatsApp has introduced a report button in the app. WhatsApp receives when a report is made using the button, the last five messages sent by that person in a "decrypted" form.

**Q7. In the case of generative Artificial Intelligence and end-to-end encryption, what are the challenges and recommended mitigation measures, including the application of advanced technology needed by technology companies, online service providers and law enforcement to prevent by blocking the sharing and removal of CSAM?**

AI-generated CSAM are synthetic images that exploit minors without real victims but perpetuate harmful behaviors and demand. Addressing this issue requires stringent regulations, advanced detection technologies, and collaborative global efforts to prevent distribution and protect children from virtual exploitation.

Challenges:

* End-to-End Encryption provides robust privacy for users, it also creates a significant challenge for law enforcement and online service providers to detect and intercept CSAM.
* Generative AI can be misused to create realistic CSAM, making it difficult to distinguish between real and AI-generated content.
* Perpetrators often use sophisticated techniques to hide CSAM, including encryption, steganography, and deepfakes, complicating detection efforts.
* The global nature of the internet means that CSAM can be hosted and shared across jurisdictions, complicating enforcement actions.

Recommended Mitigation Measures:

* Deploy advanced AI and machine learning algorithms to analyze patterns and detect potential CSAM including AI-generated content and deepfakes, even within encrypted traffic by analyzing metadata and behavioral patterns.
* Encourage cooperation between technology companies, online service providers, and law enforcement agencies to share information and best practices.
* Strengthen international legal frameworks and agreements to facilitate cross-border collaboration, enforcement of policies for ISPs to prevent the distribution of CSAM and enforcement of mandatory reporting.
* Develop and promote robust parental control tools to help parents monitor and manage their children’s online activities.
* Explore the use of advanced encryption techniques like homomorphic encryption that allow computations on encrypted data without decrypting it, enabling detection of CSAM in encrypted traffic.
* Implement real-time monitoring systems for detecting and blocking CSAM uploads and shares on platforms.

**Q8. Are there any examples of proactive measures taken to facilitate consultation and participation with a broad range of stakeholders, including children and child- rights organisations, for informing policy and legislation, setting technical standards and implementing processes to eradicate child sexual abuse and exploitation in the digital environment?**

Yes, at national and state-level in India, ICP has conducted a series of consultations with an aim to build a synergy between various stakeholders, robust accountability mechanism and pave a strong way for tackling OCSA and creating a safer digital environment. The consultation facilitated ideation and deliberation for the state child protection agencies for developing and implementing robust action plan for prevention, enhancing reporting, investigation of CSAM cases, and rehabilitation of victims.

A National Symposium was organized to address the critical themes related to promoting child rights in the digital realm, encompassing areas like online safety education, parental guidance and support in the digital age, preventing child abuse, cyberbullying & online harassment, and enhancing digital literacy.

Internationally, proactive measures against OCSA includes:

* The Budapest Convention, which harmonizes laws and enhances cooperation among nations.
* The Optional Protocol to the Convention on the Rights of the Child supplements child protection measures by addressing the sale of children, child prostitution, and child pornography.
* The WePROTECT Global Alliance unites governments, the private sector, and civil society to develop coordinated responses to combat online exploitation.
* The Global Partnership to End Violence Against Children emphasizes child participation in decision-making processes, ensuring policies are informed by their perspectives.
* Tech Coalition, comprising major technology companies, collaborates with child-rights organizations to develop technologies and policies aimed at eradicating OCSA, collectively working towards safeguarding children from online exploitation.

**Q9.What kind of mechanism could be put in place to best support and coordinate the joint public and private industry participation at the international level on existing and emerging threats that digital technologies pose to children in order to ensure harmonisation and mainstreaming across domestic and regional efforts when combatting this phenomenon?**

To effectively combat online threats to children and ensure harmonized international efforts, the establishment of a Global-level Child Online Safety Alliance (mechanism) / Regulatory Body (with corresponding national bodies) is proposed. This alliance would bring together national governments, international organizations, tech companies, and Civil Society Organizations under a standardized structure. There should be a global convention to end OCSA.

Key functions would include

1. Development of harmonized legal frameworks and technical standards
2. Alignment and standardization of international norms, judicial framework and State legislations
3. Nations to develop a mechanism for real time tracking of OCSA cases
4. To facilitate real-time data exchange
5. Formulation of task force at national and international level
6. Coordination, cooperation and convergence for regulating, monitoring and investigating purposes
7. Development of forensic tools, software, web crawlers for identification and monitoring of OCSA content
8. Capacity building and knowledge sharing for investigating and prosecuting agencies
9. Comprehensive victim support services
10. Organize consultations and events for convergence among stakeholders