# National Human Rights Commission

## Advisory for Protection of the Rights of Children against Production, Distribution and Consumption of Child Sexual Abuse Material (CSAM)

Advancements in Information and Communications Technology (ICT) provide optimal conditions for creating an ecosystem that supports proliferation of Child Sexual Abuse Material (CSAM). While role of the Internet in modern society is that of an indispensable positive social force, it cannot be denied that in few areas, like child sexual abuse, it has enabled significant harm. Production, distribution and consumption of CSAM is one of the most terrible forms of sexual abuse and exploitation faced by children and, consequently, a grave violation of their human rights. Statistics indicate a colossal rise in the proliferation of CSAM across the globe. According to the National Center for Missing and Exploited Children (NCMEC) 'CyberTipline 2022 Report', out of the 32 million reports received by NCMEC, 5.6 million reports pertained to CSAM uploaded by perpetrators based out of India. A total of 1,505 instances of publishing, storing and transmitting CSAM under Section 67B of Information Technology (IT) Act, 2000 and Sections 14 and 15 of the Protection of Children from Sexual Offences (POCSO) Act, 2012 had been reported in the year 2021.

Production of CSAM creates a permanent record of sexual abuse while its subsequent transmission and consumption via Internet and other means results in perpetual victimization of children thereby having a lasting psychological impact on the child leading to further disruption of his/ her overall development. Effective identification and blocking of CSAM content, timely sharing of data among stakeholders and expedited prosecution of offenders is the need of the hour. However, it is easier said than done as the discourse surrounding the human rights and dignity of children is intertwined with issues relating to right to privacy of individuals in the digital environment. In this regard, the role of various national as well as international stakeholders, including governments, law enforcement agencies, Internet intermediaries and civil society, is indispensable in effectively collaborating and curbing this menace.

The Government of India has ratified the United Nations Convention on the Rights of the Child (1989) and its Optional Protocol on the 'Sale of Children, Child Prostitution and Child Pornography' (2002). The Information Technology (IT) Act, 2000 and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 along with the Protection of Children from Sexual Offences (POCSO) Act, 2012 and the POCSO Rules, 2020, the Indian Penal Code, 1860 and the Juvenile Justice (Care and Protection of Children) Act, 2015 constitute the legal framework for addressing CSAM. The Government of India, through NCRB, has signed a Memorandum of Understanding (MOU) with National Centre for Missing and Exploited Children (NCMEC), a non-profit organisation in USA, for receipt of Cyber

Tipline Reports (CTRs) on CSAM from the latter. The CTRs received by NCRB are shared with the respective States/ UTs online via National Cybercrime Reporting Portal for further action. The Cyber Crime Prevention against Women and Children (CCWC) scheme for capacity building of Law Enforcement Agencies (LEAs) and the Indian Cyber Crime Coordination Centre (I4C) scheme for coordinating compliances, undertaking R&D activities and all-India drives against CSAM have been launched. Lastly, the Supreme Court of India had constituted a committee of experts to assist and advise it on feasibility of ensuring that CSAM and Rape/ Gang Rape (RGR) content is not made available to general public.

The National Human Rights Commission is mandated under Section 12 of the Protection of Human Rights Act, 1993 to protect and promote human rights of all persons, including children. The Commission has endeavoured to protect the human rights of children in the digital environment. Now, the Commission issues the following Advisory, consisting of four parts, to supplement the efforts of the Government in ensuring the protection of rights of children vis-à-vis proliferation of online CSAM. Part I deals with addressing legal gaps and issues of harmonization of laws pertaining to CSAM. Part II contains measures for monitoring and regulating Internet intermediaries, including use of technology to monitor CSAM content online, sharing of information and cooperation with the Government. Part III pertains to creation of a specialized mechanism of law enforcement for addressing CSAM as well as strengthening the existing mechanism involved in detection, investigation and monitoring of CSAM. Lastly, Part IV recommends measures for capacity building and training of officials, sensitization, awareness and support to survivors of CSAM.

## I. Legal challenges and addressing the gaps

1. Terminology:

   a.) The phrase "Child Pornography" in Section 2(1) (da) of the POCSO Act, 2012 should be replaced with "Child Sexual Abuse Material" (CSAM). Terms like "use of children in pornographic performances and materials", "child sexual abuse material" and "child sexual exploitation material" to be preferred over "Child Pornography".

   b.) The term "sexually explicit" needs to be defined under Section 67B of the IT Act, 2000 to ensure prompt identification and removal of online CSAM.

2. Definition of Intermediary: The generic definition of "intermediary" under Section 2 (w) of the IT Act, 2000 should expressly include Virtual Private Network (VPN) service providers, Virtual Private Servers (VPS) and Cloud Service Providers to avoid ambiguity and reinforce compliance of the CSAM related provisions of the IT Act by them.

3. Harmonization of laws: Harmonization of laws across jurisdictions through bilateral agreements may be explored as CSAM might be created, uploaded, shared and viewed from multiple jurisdictions.

4. International Treaty: Government of India (GOI) to pursue the adoption of UN draft Convention on 'Countering the Use of Information and Communications Technologies for Criminal Purposes', containing provisions pertaining to addressing CSAM and cyber grooming, by the General Assembly.

5. Enhancing punishment: Considering the gravity of the offence, the current quantum of punishment for offences pertaining to online CSAM under Section 14 of the POCSO Act and Section 67B of the IT Act (seven years or less) may be relooked or exempt the application of Section 41A CrPC by making appropriate legislative changes.

6. Certificate under Section 65B of the Indian Evidence Act: The requirement of issuing a certificate under Section 65B of the Indian Evidence Act, 1872 in online CSAM may be relooked in cases relating to CSAM to prevent delay in investigation.

**II. Monitoring and regulating intermediaries**

1. Use of technology: Intermediaries, including Social Media Platforms, Over-The-Top (OTT) applications and Cloud Service Providers, must deploy technology, including content moderation algorithms, to proactively detect CSAM on their platforms and remove the same. Similarly, platforms using End-to-End Encryption services may be mandated to devise additional protocols/ technology to monitor circulation of CSAM. Failure to do so to invite withdrawal of 'safe harbour' clause under Section 79, IT Act, 2000.

2. CSAM specific policy: Intermediaries be mandated to develop a CSAM specific policy that clearly outlines a user-friendly in-house reporting mechanism, notification of a dedicated point of contact (the details of which may be adequately advertised), standardized response time (considering the speed of circulation of online CSAM) and use of technology for detection and removal of CSAM from their respective platforms. The said policy should be made in consultation with Government and conveyed to the users by prominently displaying the same.

3. Removal of CSAM: Considering the speed of circulation of online CSAM, the time taken for removal of content by Intermediaries after getting information from appropriate government/ authorized agencies should not be more than 6 hours, as against 36 hours under Rule 3 (1) (d) of the Intermediary Guidelines, 2021. Further, de-indexed content must be removed every time it resurfaces without another authorization for the same.

4. Partnerships: Intermediaries must explore having partnerships amongst themselves to enable sharing of real time information pertaining to CSAM content detected on their platforms in the same way as they share data for advertising. On receipt of the same, the recipient intermediary must remove the said content.

5. Information-sharing: Intermediaries should be directed to share information regarding CSAM content detected on their respective platforms with NCRB/ any

other GOI mandated authority. Presently, Intermediaries share CSAM content with NCMEC, USA, which, in turn, shares it with NCRB.

6. Pop-up messages: ISPs, web browsers and OTT players to ensure that pop-up warning messages are displayed for searches related to CSAM.

7. Availability of records: ISPs to ensure maintenance of complete Internet Protocol Detail Record and IPDR (with destination Internet Protocol, IP/ Port) of specific Internet connections/ source IP/ destination IP. Moreover, in case a subscriber shifts from one IP to another, the earlier ISP should maintain the history of Internet connection for at least one year. The ISPs should provide requisite data to LEAs in a reasonable time frame, particularly in CSAM related crimes.

8. KYC and availability of records: ISPs and intermediaries to ensure compliance of KYC norms of their subscribers and easy traceability and availability of records for use by LEAs in CSAM related crimes.

9. Domain registration: Ensure compliance of KYC norms in the domain registration process. This be particularly applied to the registrants of .in domain names, including entities based abroad. NiXi (National Internet Exchange of India), which maintains the .in Registry, should develop a web portal enabling LEAs to easily access the registration details of .in domains.

10. Quarantining posts to enable technology/ Artificial Intelligence (AI) to detect CSAM before publishing must be made mandatory.

11. Certificate for digital evidence: Ensure Social Media Platforms, including those based abroad, provide a certificate for producing Digital Evidence of online content u/s 65B of the Indian Evidence Act. Presence of Social Media Intermediaries (SMIs) in courts during trial through Grievance Officer to be ensured.

12. Cooperation with the Government: Government of India should develop a uniform format to seek data from intermediaries which can be used by the LEAs, in consultation with them. Grievance Officer of Intermediaries be held responsible for providing requisite data as evidence to the LEAs in a time bound manner, instead of seeking the same through the Mutual Legal Assistance process.

13. VPN Regulations: Since VPN allows obfuscation of identity of users, ISPs may use Deep Packet Inspection (DPI) to analyze the packets passing through their network to identify the details of VPN users, which should be provided to the respective LEAs, particularly in cases relating to CSAM. Ensure compliance of the Notification dated 28.04.2022, titled 'Directions under sub-section (6) of section 70B of the IT Act, 2000, relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe and Trusted Internet' (VPN Regulations) by the ISPs.

## III. Detection, investigation and monitoring of CSAM

1. Specialized State Police Units: Every State/ UT to have at least one Specialized State Police Unit for detection and investigation of CSAM related cases and apprehension of offenders. The Government of India to assist the setting up and equipping these units, for instance, through grants under Modernization of State Police Forces (MPF) Scheme, Police Technology Mission and Nirbhaya Fund.

2. Specialized Central Police Unit: A Specialized Central Police Unit in the GOI to deal with CSAM related matters, including detecting CSAM content, maintaining its repository, analyzing patterns, assisting investigative agencies, initiating the process for takedown of content and so forth, be established. It should consist of experts in identification and investigation of CSAM in order to focus on identifying and apprehending CSAM offenders both in dark web and open web and developing a comprehensive and coordinated response of investigation and law enforcement agencies towards monitoring, detection and investigation of CSAM.

3. Nodal Point: The proposed Specialized Central Police Unit should also act as a nodal point for collaboration with stakeholders, international cooperation, liaison with LEAs of states, coordination of all-India drives against CSAM, generation of awareness and creation of deterrence. It will also keep a track of the national database of hash values of known CSAM and manage blocking of the same by intermediaries.

4. Database of CSAM:

   a.) A national database of CSAM with hash values of known CSAM be created by the proposed Specialized Central Police Unit so that the required content be blocked by intermediaries. This should be maintained by the proposed Specialized Central Police Unit.

   b.) The proposed Specialized Central Police Unit must ensure collection of disaggregated data pertaining to prevalence, trends, and patterns of CSAM, involving gender, age, caste, ethnicity, or other socio-economic parameters to better understand the issue and inform policy-based interventions.

   c.) NCRB receives Cyber Tipline Reports (CTRs) from the NCMEC, USA, which are transmitted to the concerned state Police. This data be maintained in a structured form to enable search and analytics.

   d.) The Central Bureau of Investigation (CBI) has access to the International Child Sexual Exploitation (ICSE) database maintained by INTERPOL. Access of the same may be shared with NCRB (since it already receives similar reports from NCMEC) for forwarding the same to all state Police.

   Alternatively, access to the ICSE database may be provided to all states for reducing delays in investigation. However, as a prerequisite, the state Police may

be required to set up ICT enabled Specialized State Police Units for CSAM related investigations.

e.) The National Database on Sex Offenders maintained by NCRB, MHA, be expanded to include CSAM offenders convicted under Section 67B, IT Act, 2000 and Sections 14 and 15, POCSO Act, 2012.

f.) A separate dashboard on CSAM related offences be incorporated in the Inter-Operable Criminal Justice System (ICJS)/ Crime and Criminal Tracking Network & Systems (CCTNS) database which is used by NCRB for Investigation Tracking System for Sexual Offences (ITSSO).

5. Reporting Portal (www.cybercrime.gov.in): The requirement of uploading a valid national ID of the victim under the 'Report and Track' feature be done away with as the identity of the victims may not be known in many instances.

6. Use of technology

a.) The Specialized Central and State Police Units should use technological methods like hotspot mapping, predictive policing, Geographic Information System (GIS), and identity resolution to identify repeat offenders and alert potential victims of online child sexual abuse, for instance, in cases of suspected online grooming.

b.) Government to direct and incentivize development of indigenous technological tools to detect CSAM, for instance, by organizing hackathons or through grants under Modernization of State Police Forces (MPF) Scheme, Police Technology Mission and Nirbhaya Fund. Pertinently, some cloud Application Programming Interface (API) based software tools are being used by Intermediaries, including, CloudFlair, Safer, Google's AI tool, Griffeye, etc., to detect CSAM on their platforms.

c.) Registrants of .in domain names be mandated to have in-built software for proactively detecting CSAM before the same is uploaded on the portal.

d.) NCRB should develop software for auto-resolution of IP Address, date and time from Cyber Tipline Reports (CTRs) received by it from NCMEC. Until then, one may consider using foreign software tools like the Internet Crimes Against Children Child On-line Protection System (ICACCOPS) for monitoring CSAM.

7. Repository of software tools: Develop a national repository of software tools, including tools for scanning of CSAM, extracting IP address, etc., to be made available for use by LEAs. Pertinently, the NCRB is in the process of developing a tool to address manual scanning of CSAM because the latter can overwhelm the investigators.

8. Forensic investigators: The number of forensic investigators needs to be substantially increased because online child abuse related cases are proliferating. Since proliferation of CSAM is a specialized crime, forensic investigators and examiners entrusted with such cases must also be proficient to handle them.

9. General Consent to CBI: It takes considerable time in receiving consent for CBI investigation from the concerned State as there is no general consent to CBI for investigation by most of the states. States should give consent for investigation by CBI of cases pertaining to online CSAM under the IT Act, 2000 and the POCSO Act, 2012.

10. Monitoring and evaluation: Mechanisms to continuously monitor and evaluate the effectiveness of policy interventions pertaining to CSAM be established by the proposed Specialized Central Police Unit to identify gaps to enable improvement of the same.

**IV. Capacity building, sensitization, awareness and victim support**

1. Training courses and sensitization of officials:

   a.) The National Cybercrime Training Centre (CyTrain) portal to devise a training course/ Standard Operating Procedure (SOP) for investigation and disposal of CSAM related cases by LEAs, public prosecutors and judges. This should be regularly upgraded with evolving technology.

   b.) Officials of the state Police managing the CTRs be provided technical training to handle the same.

   c.) Police officials dealing with cases pertaining to CSAM to be imparted sensitization training on rights of children in the digital environment, their specific vulnerabilities on the Internet, the extent and emerging manifestations of CSAM and the use of child-friendly procedures in investigation.

   d.) States to take up capacity-building programmes for Police forces to effectively address cyber crimes against children, including cyber exploitation and CSAM.

2. Awareness and sensitization of parents, children: Schools, colleges and institutions to ensure continuous education and generation of awareness among students, parents and teachers on the modus operandi of online child sexual abusers, specific vulnerabilities of children online, reporting mechanisms, recognizing early signs of online child abuse and grooming through emotional and behavioural indicators, use of parental control apps, Internet safety among children through different means, like conducting workshops in schools, involving civil society, etc.

3. Cyber curriculum: Central and State Education Boards to draft and incorporate cyber curriculum in schools, including cyber safety, personal safety, relevant child care legislation (including Section 67B, IT Act, 2000 and Sections 11, 13, 14 and 15, POCSO Act, 2012), national/ local policies and legal consequences of violating the same, etc.

4. Psycho-social care and support: Survivors of CSAM be provided support services and opportunities for rehabilitation through various means, like partnerships with civil society and other stakeholders. Psycho-social care centres may be established in every district to facilitate need-based support services and organization of stigma eradication programmes.

5. Lexicon in vernacular languages:

   a.) Encourage development of cyber security lexicon in languages other than English so that people are well educated and aware of the same.

   b.) Lexicon used to search CSAM online be translated into vernacular languages. It may be used to develop algorithms to detect CSAM shared online in vernacular languages.

6. Recurring SMS services: SMS alerts to be sent to every mobile phone through Telecom Service Providers every quarter/ month cautioning users about CSAM.

7. Chief Information Security Officers: The Chief Information Security Officers (CISOs) of organizations should be sensitized to proactively identify cases where CSAM is stored or accessed in their respective organizations.

****

**Annex**

**List of Some Abbreviations**

| | | |
|---|---|---|
| CBI | - | Central Bureau of Investigation |
| CSAM | - | Child Sexual Abuse Material |
| CTR | - | Cyber Tipline Report (received by NCRB from NCMEC) |
| GoI | - | Government of India |
| I4C | - | Indian Cyber Crime Coordination Centre |
| ICT | - | Information and Communications Technology |
| IO | - | Investigating Officer |
| IP | - | Internet Protocol |
| ISP | - | Internet Service Provider |
| IT | - | Information Technology |
| LEA | - | Law Enforcement Agency |
| MeitY | - | Ministry of Electronics and Information Technology |
| MHA | - | Ministry of Home Affairs |
| MWCD | - | Ministry of Women and Child Development |
| NCMEC | - | National Center for Missing and Exploited Children |
| NCRB | - | National Crime Records Bureau |
| NGO | - | Non-Governmental Organization |
| OTT | - | Over-The-Top |
| POCSO | - | Protection of Children from Sexual Offences |
| SOP | - | Standard Operating Procedure |
| VPN | - | Virtual Private Network |

***