**Request for inputs for the thematic report of the UN Special Rapporteur (SR) on the sale,**

**sexual exploitation and sexual abuse of children**

 **“Existing and Emerging Sexually Exploitative Practices against Children In the Digital Environment.”**

| **NO.** | **KEY QUESTIONS AND INPUTS SOUGHT** | **INPUTS BY LINE AGENCIES** |
| --- | --- | --- |
|  | Please provide information on how technologies are used to facilitate the sexual exploitation and abuse of children. | Technologies facilitate the sexual exploitation and abuse of children through social media, messaging apps, and online gaming platforms where predators groom and manipulate victims. The dark web and encrypted communications help distribute child sexual abuse material (CSAM) anonymously, while live streaming services broadcast abuse in real-time. File-sharing services and cloud storage are used to store and share CSAM, and VPNs and encryption mask predator activities. AI technologies, including deepfakes, further exacerbate the problem.  |
|  | What practical recommendations would you propose for States, the technology industry and online service providers to prevent sexual exploitation and abuse of children in the digital environment? | To prevent the sexual exploitation and abuse of children online the technology industry should invest in AI to detect abuse, implement user verification, enhance reporting mechanisms, integrate privacy and safety features, and maintain transparency. Online service providers need to employ content moderation, educate users on safety, collaborate with authorities, conduct regular security audits, and promote safe interactions on their platforms. Through these combined efforts, a safer digital environment for children can be achieved.As the regulator of the communications and multimedia industry in Malaysia, the Malaysian Communications and Multimedia Commission (MCMC) enforces the Communications and Multimedia Act 1998 (CMA 98) and takes actions against online content that are obscene, indecent, false, menacing, offensive in nature. In collaboration with the Royal Malaysian Police, MCMC works to block websites and take down social media content involving child sexual abuse materials (CSAM) as well as pornographic materials from the online environment in Malaysia.  |
|  | 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? | Technology companies may lack robust detection and reporting tools, user verification processes, and effective content moderation. Privacy concerns and the anonymity of the Internet also hinder efforts to track and prosecute offenders. These gaps collectively limit the effective implementation and application of existing laws and policies to protect children online.Websites that are hosted in other countries pose cross border issues such as jurisdictions of international law and international collaborations. Questions arise about which country’s laws apply when a website operates globally. Factors like the location of servers, users, and content creators all come into play. Addressing cross-border issues requires collaboration among regulatory bodies, law enforcement agencies, and industry stakeholders.The Malaysian Communications and Multimedia Commission (MCMC) provides technical assistance such as suspects profiling to the Royal Malaysian Police for investigation purposes.  |
|  | 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? | Investigating, detecting, and prosecuting child sexual abuse materials (CSAM) online is a critical task to ensure justice is served to both the survivor and perpetrator. Several challenges hinder the law enforcement efforts across jurisdictions.1. **Anonymity and Encryption**

Predators use encryption and anonymizing tools like VPNs and the dark web to hide their identities and activities, making it difficult for law enforcement to trace and identify them.1. **Jurisdictional Issues**

The global nature of the internet means that perpetrators, victims, and digital evidence can be spread across multiple countries, complicating jurisdiction and legal authority for investigations and prosecutions. 1. **Resource Constraint**

Law enforcement agencies often lack the resources, specialized training, and advanced technology needed to effectively track, investigate, and remove child sexual abuse material (CSAM) online.1. **Rapidly Evolving Technology**

The fast pace of technological advancements outstrips the ability of laws and law enforcement practices to keep up, leading to gaps in regulation and enforcement capabilities.1. **Data Privacy Laws**

Strict data privacy regulations can limit law enforcement’s ability to access necessary data and cooperation from tech companies, hindering investigations and evidence gathering.1. **Inadequate Reporting Mechanism**

Online platforms may have insufficient or ineffective reporting and content moderation systems, delaying the identification and removal of CSAM.1. **Volume and Variety of Content**

The sheer volume of data and content shared online makes it challenging for law enforcement to monitor, detect, and act on every instance of CSAM and related criminal activities. |
|  | 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 with online child sexual exploitation and abuse, and ensuring the minimum harmonization across legal jurisdictions? | States, the technology industry, and online service providers can implement the following technical and regulatory measures to mitigate human rights risks associated with online child sexual exploitation and abuse, and ensure the minimum harmonization across legal jurisdictions:1. **Technology Industry**
2. Invest in and deploy AI and machine learning tools to detect and remove child sexual abuse material (CSAM). Regularly update these tools to keep up with evolving threats and tactics. Implement robust user verification processes to reduce anonymity and deter potential offenders. Use multi-factor authentication and other security measures to ensure user authenticity.
3. Create and promote easy-to-use tools for users to report suspicious activities and CSAM. Ensure that reported content is promptly reviewed and actioned.
4. Implement age-appropriate settings, parental controls, and automatic content moderation.
5. Publish regular transparency reports on measures taken to combat online child exploitation and their effectiveness.
6. **Online Service Providers:**
7. Employ dedicated teams and technologies to monitor and promptly remove CSAM. Utilize AI tools to assist human moderators in identifying and actioning harmful content.
8. Provide resources and safety tips for users, particularly children and parents, on how to stay safe online. Offer training sessions and workshops on digital literacy and online safety.
9. Establish clear protocols for cooperation with law enforcement agencies, including timely sharing of information and data when legally required. Participate in joint efforts and initiatives to combat online child exploitation.
10. Design platform features that encourage safe and positive interactions among users. Implement robust privacy controls, anti-abuse features, and support for users experiencing online abuse.
11. Close collaborations with law enforcement to understand the techniques deployed by predators.
12. **Harmonization Across Jurisdictions**
13. Develop and adopt international standards and guidelines for online safety and child protection. Ensure these standards are aligned with human rights principles and best practices.
14. Work towards harmonizing laws and regulations across countries to facilitate coordinated enforcement and prosecution. Participate in international treaties and conventions that address online child exploitation.
15. Create and maintain international databases of known offenders and CSAM to aid in cross-border investigations and enforcement. Ensure these databases are accessible to authorized personnel while maintaining strict data protection standards.
16. Organize international training programs for law enforcement, judiciary, and technology professionals. Facilitate knowledge exchange and capacity-building across jurisdictions.
 |
|  | 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? | The Malaysian Communications and Multimedia Commission (MCMC) conducts proactive monitoring for online content that is in breach of the Communications and Multimedia Act 1998, which is obscene, indecent, false, menacing, and offensive in nature. In collaboration with the Royal Malaysian Police, MCMC works to block websites and take down social media content involving child sexual abuse materials (CSAM) as well pornographic materials from the online environment in Malaysia. In addition, MCMC provides technical assistance such as suspects profiling to RMP for investigation purposes. Internet users in Malaysia can lodge complaints, including online content related issues, to MCMC through the official complaint channel at <https://aduan.mcmc.gov.my>  |
|  | 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 child sexual abuse material (CSAM)? | **Challenges**1. End-to-End Encryption is essential for privacy but it can prevent service providers from detecting and removing CSAM. Encryption and anonymization tools hinder the identification of offenders.
2. The sheer volume of data shared online makes it difficult to monitor and identify CSAM in real-time. Encrypted platforms can facilitate the rapid spread of CSAM, making timely intervention challenging.

**Recommended Mitigation Measures**1. Online service providers to provide technical support in evidence gathering and investigation of online child sexual abuse cases.
2. Implement scanning mechanisms e.g., algorithm, to detect CSAM before content is encrypted which can be done at the client-side or during the upload process. The system should be able to trigger law enforcement agencies for immediate actions to be taken.
3. Develop and deploy advanced AI models trained to detect synthetic CSAM and deepfakes. These models should be regularly updated to stay ahead of new AI-generated threats.
4. Use metadata and behavioural analysis to identify suspicious activities and patterns indicative of CSAM sharing. Implement anomaly detection systems that flag unusual behaviour that may indicate the distribution of CSAM.
5. Encourage and simplify user reporting of suspicious content. Provide clear and easy-to-use reporting tools. Use automated systems to generate alerts for potential CSAM based on predefined criteria and user reports.
6. Participate in industry-wide coalitions and share information on new threats, detection methods, and best practices.
7. Online service providers establish protocols for timely sharing of critical information with law enforcement agencies.
 |
|  | 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? | The Malaysian Communications and Multimedia Commission (MCMC) actively addresses child sexual abuse and exploitation in the digital environment. While specific technical standards are not explicitly mentioned, MCMC collaborates with various stakeholders to combat online threats, including child sexual exploitation. Initiatives such as the Klik Dengan Bijak (English- Click Wisely) and the Malaysian ICT Volunteer promote safe online behaviour, and the MCMC restricts access to websites containing child sexual abuse content through collaboration with Interpol and the Royal Malaysia Police. Although detailed technical standards are not specified, the MCMC’s efforts focus on creating a safer online space for children. |
|  | 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 support and foster close collaboration between public and private sectors at the international level in combating existing and emerging threats posed by digital technologies to children, a comprehensive mechanism can be established with the following components.:1. Develop a global action plan that outlines clear objectives, strategies, and timelines for addressing online child exploitation. Ensure all participating countries and organizations commit to the action plan and regularly review progress.
2. Form joint task forces with members from different countries and sectors to tackle specific issues related to online child exploitation. Assign task forces to specific missions, such as dismantling dark web networks, developing new detection technologies, or coordinating large-scale operations.
3. Establish standardized protocols and guidelines for detecting, reporting, and prosecuting online child exploitation cases. Ensure all participating entities adhere to these standards to maintain consistency and effectiveness.
4. Organize joint training programs for law enforcement, judiciary, tech industry employees, and NGOs. Focus on building capacity in areas such as advanced detection technologies, forensic analysis, and victim support.
5. Encourage the sharing of technology, expertise, and resources to enhance detection, reporting, and removal of child sexual abuse material (CSAM).
 |

**Prepared by:**

**The Government of Malaysia**