Child Sexual Abuse Material Related to Cyber Domain

What is CSAM?

Child sexual abuse material (CSAM) refers to sexually explicit content involving a child. Visual depictions can include photographs, videos, or computer-generated images indistinguishable from a specific minor.

There are various terms used across the globe to describe this material, including:
- ✓ CSAI — child sexual abuse imagery
- ✓ CSEI — child sexual exploitation imagery
- ✓ IIOC — indecent images of children

While U.S. federal law still refers to this material as "Child Pornography," **CSAM is now the preferred language**, and efforts are underway in many jurisdictions to update the terminology in legal guidelines.

CSAM is a recorded copy of the abuse, be it sexual, physical, mental, social, or emotional, permanently made available over the vast internet. With the technological boom, it becomes easier for offenders to photograph, record, or watch live CSA; store CSAM on the device; access CSAM stored remotely; connect with victims and other offenders; and distribute and receive CSAM through an endless variety of applications. This network is so sophisticated that it encrypts all messages and devices, providing a false sense of security to offenders.

India, with its vast population and rapid technological growth, has faced significant challenges in combating the spread of Child Sexual Abuse Material (CSAM) online. The country's large internet user base and the widespread availability of smartphones have made it a fertile ground for the production, distribution, and consumption of this harmful content. Child Sexual Abuse Material (CSAM) is a critical issue in the cyber domain, and India has been actively working to combat it through various measures.

Definition

CSAM includes any visual depiction of sexually explicit conduct involving a minor. This can be photos, videos, or digital images.

Differences between CSAM and Child Pornography

Many people use the terms CSAM and child pornography interchangeably, but there are key differences. Child Sexual Abuse Material, or CSAM, refers specifically to images, videos, and other media that document the sexual abuse of children.

This definition is broad and includes all forms of child exploitation.

On the other hand, child pornography has a more narrow focus. It usually refers to material that sexually exploits children for the purpose of adult sexual gratification. All CSAM is illegal and harmful.

What are the materials typically included in Child Sexual Abuse Materials (CSAM)?

a. **Images:** Photographs or digital images that depict children in sexually explicit poses or activities. The digital world makes it quite easy to gather and transmit images, thus jeopardising the lives of children.

b. **Videos:** Recorded footage showing children being subjected to sexual acts or abuse. As gruesome as it sounds, it is true.

c. **Live-streamed content:** Real-time video broadcasts capturing the sexual exploitation of children as it happens.

d. **Written narratives:** Stories or text-based content that describes sexual abuse scenarios involving children in detail. Some offenders might be interested in such stories or texts.

e. **Drawings and animations:** Graphic depictions or animations portraying children in sexual situations. Unfortunately, these expressive forms of communication are often misused to portray children in inappropriate scenarios.

f. **Advertisements and solicitations:** Online promotions or solicitations promoting the exchange or sale of CSAM. They infamously popularise the CSAM to target its viewer audience.

g. **Chat logs and conversations:** Communications discussing or arranging the exchange of CSAM. The administrator of such discussions is often the person who kick-starts the heinous crime.

h. **Websites and online forums:** Online platforms dedicated to the distribution, sharing, or discussion of CSAM. They provide a breeding ground for the exchange of illegal material.

i. **Sextortion materials:** Content obtained through the extortion of sexually explicit material from children. Children are often blackmailed into sharing such content, leading them into a trap of abuse. It is appalling, yet a reality.

j. **Compilation albums:** Collections of CSAM categorised by age, gender, or type of abuse.

Distribution Channels

CSAM is often distributed through various online platforms, including social media, file-sharing networks, and encrypted messaging apps.

Creation and Perpetrators

The majority of those creating and distributing CSAM also commit hands-on sexual offenses against minors. Offenders often use grooming techniques to normalize sexual contact and encourage secrecy.

Artificial Intelligence (AI) and the Production of Child Sexual Abuse Imagery

The Internet Watch Foundation (IWF) has identified a significant and growing threat where AI technology is being exploited to produce child sexual abuse material (CSAM). AI-generated imagery of child sexual abuse has progressed at such an accelerated rate that the IWF is now seeing the first realistic examples of AI videos depicting the sexual abuse of children.

These incredibly realistic deepfake (media (images, videos, or audio) that has been digitally manipulated through AI tools or software to replace one person's likeness convincingly with that of another), or partially synthetic, videos of child rape and torture are made by offenders using AI tools that add the face or likeness of a real person or victim.

Key Takeaways

Increase in AI-generated Child Sexual Abuse Material: The latest findings show over 3,500 new AI-generated criminal child sexual abuse images have been uploaded on to the same dark web forum as previously analysed in October 2023.

More Severe Images: Of the AI-generated images confirmed to be child sexual abuse on the forum, more images depicted the most severe Category A (IWF classifies the 'severity' of abuse, with Category A material containing the most severe kinds of sexual abuse) abuse, indicating that perpetrators are more able to generate complex 'hardcore' scenarios.

Emergence of AI Child Sexual Abuse Videos: AI-generated child sexual abuse videos, primarily deepfakes, have started circulating, highlighting rapid technological advancements in AI models/generators. Increasingly, deepfake videos shared in dark web forums take adult pornographic videos and add a child's face using AI tools.

Clear Web Increase: There is a noticeable increase in AI-generated child sexual abuse imagery on the clear web, including on commercial sites.

AI Child Sexual Abuse Featuring Known Victims and Famous Children: Perpetrators increasingly use fine-tuned AI models to generate new imagery of known victims of child sexual abuse or famous children.

Victims

Victims range from infants to teenagers, with a significant portion being prepubescent children. The abuse depicted in CSAM is often severe, with 84.2% of videos and images containing extreme abuse.

Impact

CSAM has a profound and lasting impact on victims. It serves as a record of a child's abuse and can be used to revictimize and stalk victims long after the original abuse.

Causes of Child Sexual Abuse Material (CSAM)

1. **Market Demand:**
   Individuals with a sexual interest in children drive demand for new and more egregious images, perpetuating abuse. The push for new CSAM results in the continued abuse and exploitation of child victims, and the abuse of new children every day.

2. **Grooming of Minors:**
   Perpetrators increasingly groom minors for sexually explicit conduct online, exploiting vulnerabilities. Offenders have been known to take advantage of multiple vulnerabilities of a child, including a minor's fear of getting in trouble with their parents or guardians, school, or law enforcement.

3. **Lack of Parental Awareness and Technological Exposure:**
   Children's comfort with technology leaves them vulnerable, as parents may not understand online activities or available protection measures.

4. **Extortion and Blackmail:**
   Offenders take advantage of a child's fear, extorting or blackmailing them to create additional CSAM or pay a ransom.

5. **Fear of Law Enforcement:**
   Many child victims don't report abuse promptly because offenders manipulate victims, threatening police involvement and hindering reporting. Even families who are aware of the issue are concerned that the child will get into trouble with law enforcement and may not report the crime, preventing investigators from identifying and stopping the offender.

6. **Perpetual Victimisation:**
   Posting and disseminating CSAM online leads to lifelong re-victimization for children, impacting them perpetually. Victims experience double victimisation, suffering each time their abuse images are viewed, resulting in profound feelings of guilt, shame, and blame.

Increase in Cases

1. **Pandemic Surge:** During the COVID-19 pandemic, there was a notable increase in the circulation of CSAM. For instance, in Kerala, the increase was reported to be between 200% to 300% compared to pre-pandemic levels.

2. **National Statistics:** In 2020, the National Crime Records Bureau (NCRB) registered 43,000 offenses under the Protection of Children from Sexual Offences (POCSO) Act, averaging one case every 12 minutes.

Recent Reports

1. **2023 Data:** The National Human Rights Commission (NHRC) reported a 250-300% increase in CSAM on social media in India. In 2023 alone, there were approximately 450,207 cases reported.

2. **Interpol Data:** Between 2017 and 2020, India reported over 2.4 million instances of online child sexual abuse, with 80% of the victims being girls below the age of 14.

CSAM cases in India:

Kerala (2021):

'Operation P-hunt' by Kerala Police led to the arrest of 100 individuals for CSAM-related offenses, showcasing the increasing focus of law enforcement agencies on tackling CSAM.

Delhi (2022):

Delhi Police arrested an individual for sexually assaulting a minor and live-streaming it on social media, highlighting the evolving nature of CSAM.

Uttar Pradesh (2022):

A businessman was arrested for possessing and circulating CSAM on his mobile phone, illustrating the widespread nature of the issue across different demographics.

Madhya Pradesh (2023):

The National Center for Missing and Exploited Children identified over 30,000 individuals in Madhya Pradesh allegedly involved in circulating suspected CSAM, with over 4,000 cases deemed 'actionable.'

Maharashtra (2023):

'Operation Blackface' by Maharashtra Police led to the arrest of 140 individuals for CSAM-related offenses since the beginning of 2023.

Key Challenges in India

1. **Scale:** India's massive population and internet penetration make it difficult to monitor and regulate online activity.

2. **Lack of Awareness:** Many people in India are unaware of the dangers of CSAM and how to report it.

3. **Technological Limitations:** The lack of advanced technology and resources can hamper law enforcement efforts to track down perpetrators.

4. **Cultural Factors:** Certain cultural factors and societal attitudes can make it difficult to address the issue of child sexual abuse.

Here are some key aspects and initiatives related to CSAM in India:

Legal Framework

1. **Information Technology (IT) Act, 2000:** Section 67B of the IT Act provides stringent punishment for publishing, transmitting, or viewing child sexual abuse material online. Offenders can face:

   First Conviction: Imprisonment for up to 5 years and a fine up to 10 lakh.

   Subsequent Convictions: Imprisonment for up to 7 years and a fine up to 10 lakh
2. **Protection of Children from Sexual Offences (POCSO) Act, 2012:** This act specifically addresses sexual exploitation and abuse of children, including online offenses.

   The POCSO Act, designed with the best interests of children below eighteen years in mind, not only defines various offenses but also prioritizes a child's healthy physical, emotional, intellectual, and social development. A crucial aspect of the Act is the mandatory reporting of crimes, challenging the prevailing culture of silence surrounding such offenses.

a. **Defining Child Pornography (Section-2(da)):** The POCSO Act underwent a significant transformation with the introduction of Section-2(da), explicitly defining child pornography. The provision states:

   "*Child Pornography means any visual depiction of sexually explicit conduct involving a child, which includes photographs, video, digital, or computer-generated images indistinguishable from an actual child, and images created, adapted, or modified but appear to depict a child.*"

   This definition sets the tone for the Act's subsequent provisions, providing a clear understanding of what constitutes an offense under the purview of child pornography.

b. **Punishment for Using a Child for Pornographic Purposes (Section-14):** Section-14 addresses the gravest offenses involving the use of children for pornographic purposes. The provisions state:

i. **Section 14(1): "**Whoever uses a child or children for pornographic purposes shall be punished with imprisonment for a term not less than five years and shall also be liable to fine. In the event of a second or subsequent conviction, imprisonment for a term not less than seven years and also liable to fine."

ii. **Section 14(2):** "Whoever using a child or children for pornographic purposes under sub-section(1), commits an offence referred to in section 3 or Section-5 or Section-7 or Section-9 by directly participating in such pornographic acts, shall be punished for the said offences also under Section-4, section-6, section-8, section-10, respectively, in addition to the punishment provided in sub-Section(1)." These stringent provisions underscore the gravity of the offenses and ensure that those involved face severe consequences.

c. Punishment for Storage of Pornographic Material (Section-15): Originally focused on commercial use, Section-15 has been expanded to provide graded punishment commensurate with the level of the crime. The amended punishment includes:

i. **Section 15(1):** "Any person who stores or possesses pornographic material involving a child, but fails to delete or destroy or report the same to the designated authority, with an intention to share or transmit child pornography, shall be liable to a fine not less than Rs. 5000/-. In the event of a second or subsequent offense, a fine not less than Rs. 10,000/-."

ii. **Section 15(2):** "Any person who stores or possesses pornographic material involving a child for transmitting, propagating, displaying, or distributing in any manner at any time, except for the purpose of reporting or use as evidence in court, shall be punished with imprisonment of either description, which may extend to three years, or with fine, or with both."

iii. **Section 15(3):** "Any person who stores or possesses pornographic material involving a child for commercial purposes shall be punished on the first conviction with imprisonment of either description, not less than three years, which may extend to five years, or with fine, or with both. In the event of a second or subsequent conviction, with imprisonment not less than five years, which may extend to seven years, and shall also be liable to a fine."

3. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021: These rules require social media platforms to deploy technology to identify and remove CSAM proactively. Failure to do so can result in penalties.

4. Section 95 of The Bhartiya Nyaya Sanhita, 2023: Criminalizes the act of hiring, employing, or engaging a child to commit an offence.

Punishment:

a. The punishment for this offence is imprisonment for a term not less than three years but which may extend to ten years, along with a fine.

b. And if the offence be committed shall also be punished with the punishment provided for that offence as if the offence has been committed by such person himself.

Explanation:

a. Hiring
b. Employing
c. Engaging or
d. Using the child for sexual exploitation or **pornography**
e. Is covered within the meaning of this Section.

Government Initiatives

1. **Indian Cyber Crime Coordination Centre (I4C):** Established under the Ministry of Home Affairs, I4C provides a framework for law enforcement agencies to deal with cyber crimes, including CSAM.

2. **Cyber Crime Prevention against Women and Children (CCPWC):** This scheme includes an online National Cyber Crime Reporting Portal (www.cybercrime.gov.in) where the public can report complaints related to child pornography and other forms of CSAM.

3. **National Commission for the Protection of Child Rights (NCPCR):** The NCPCR is responsible for monitoring and ensuring the enforcement of child protection laws, including those related to CSAM. It developed "Cyber Safety Guidelines", and included these as a separate section in the 'Manual on the Safety and Security of Children in Schools' in 2017.

Measures and Strategies

1. **Automated Detection:** Social media platforms and intermediaries are required to deploy technology-based measures to proactively identify and remove CSAM.

2. **Grievance Redressal Mechanism:** The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 mandate intermediaries to adopt a robust grievance redressal mechanism for timely disposal of complaints.

3. **Public Awareness:** Efforts are being made to educate children and parents about online safety through school curriculums and public awareness campaigns.

Challenges

1. **Dark Web:** The side of the World Wide Web that is not indexed by search engines and requires specific configuration, software, or authorization to access allowing users and website operators to remain anonymous or untraceable. A significant amount of CSAM is shared on the dark web, making it difficult for law enforcement to track and intercept.

2. **Encryption and Anonymity:** While encryption protects user privacy, it also poses challenges for detecting and intercepting CSAM.

How can we prevent CSAM?

Preventing Child Sexual Abuse Material is a multifaceted approach that needs collaboration and a combination of several organizations. Government, Law enforcement, guardians, and society all need to come together to prevent CSAM.

1. **International Cooperation:** India collaborates with international organizations and other countries to combat CSAM, as the internet transcends national borders.

2. **Strategic Law Enforcement Approach:** Laws and regulations need to be enforced against the creation and distribution of CSAM. Law enforcement must continue

responding to the rising online CSAM with a multi-pronged approach. These laws must aim to identify victims and perpetrators earlier and enhance triage capabilities. Newer and more advanced technologies like artificial intelligence, machine learning classifiers, computer vision, natural language processing and hash algorithms can be utilized for the enforcement of the laws.

3. **Capacity Building:** The government provides financial assistance and training to state law enforcement agencies to enhance their capabilities in dealing with cyber crimes.

4. **Education of parents/guardians and children to prevent CSAM:** Educating both the parents and children is crucial in preventing CSAM. Parents need to be taught about how to control and set age-appropriate locks for the use of the internet by children to avoid any online interaction between the abusers and the children. Children need to be educated and trained about what to do if they receive fear-based messages from the perpetrator.

   Parents and children should be taught about dealing with mental health issues. Teenagers recently are suffering more through these mental health issues and they are more driven towards digital ways to combat the issues. They seek validation, attention and connection through social media applications. This gives a golden opportunity to the abusers to manipulate them and inappropriately use them.

5. **Engagement of Industries:** Industries play a pivotal role in preventing CSAM, especially the internet-related and technology-related industries. Companies must come up with implementations of safety measures to save the users. Companies must be transparent with what they are doing to protect children. This helps the users can have an idea of what to expect from them. The Tech Coalition is a global alliance of technology companies working together toward the safety of children online.

   Technologies have made a commitment to transparency as a part of project protection, announced in June 2020.

6. **Policies of government:** Several policies of government aimed at ensuring safety for internet users include –

a. National Commission for Protection of Child Rights – NCPCR
b. The Information Technology Act, 2000 – IT Act
c. Protection of Children from Sexual Offences – POCSO

Possession of Child Sexual Abuse Materials is not just a moral issue but a legal crime. Efforts to combat CSAM in India are ongoing and require the cooperation of technology companies, law enforcement, and international organizations to be effective. But they can not be eliminated without the active participation of every citizen. Let us all realise the depth of the issue and not let children become victims of inhumanity.