Committee: UNICEF
Topic: Strengthening criminal penalties for the distribution of child sexual abuse material through private messaging
Chair: Sophia Issabella Valdez Moreira
Moderator: Valentina Cárdenas De Lira

Overview of the Problem

The United Nations (UN) agency dedicated to children seeks to support the rights of all children, especially those most vulnerable. UNICEF works with over 190 countries as well as territories around the world to protect children and do whatever it takes to help children have the best chance to live, flourish, and reach their full potential. However, the distribution of CSAM via private messaging applications presents an urgent jurisdictional challenge for the committee.

The main stakeholders involved will be national governments, law enforcement bodies, UNICEF, United Nations Office on Drugs and Crime (UNODC), INTERPOL, technology companies, civil society organizations, child protection professionals, and survivors. All of these have roles to protect children, although their priorities may vary, for example around privacy, surveillance, punishment for criminals, and corporate responsibility.

It is a serious violation of children's rights and presents new challenges for law enforcement internationally. While digital tools allow instant global communication, they also facilitate serious harms, including the distribution of abusive material, exploitation of children, and sharing of images/videos without the victim's consent. The main issues are that different countries will have various laws, investigative powers, and punishments. However, content can be distributed online across several countries in seconds. This can make it easier for some people to abuse the differences between countries to avoid being caught. End-to-end encryption can also make it harder for a provider to identify any illegal content.

Delegates will examine how countries can implement reasonable criminal penalties and strengthen international cooperation through mechanisms such as mutual legal assistance treaties (MLATs). They will also consider how technology companies can be held accountable, how victims can receive proper protection, and how these measures can be implemented while respecting basic rights.

Introduction

Child Sexual Abuse Material (CSAM) is visual media that represents the sexual abuse or exploitation of a minor and it is preferred over child pornography as it highlights that this media shows abuse. Distribution is sending, sharing, selling and providing the material. Private messaging services are platforms where people can communicate with someone via direct messages or within closed groups. E2EE is a system designed to keep communications secure and private. This can present a challenge to investigations. When fighting these crimes, governments will set out criminal punishments, like jail, fines, or other legal actions for those found guilty. As these crimes often involve many countries, an international approach is needed to share evidence, find victims and punish the offenders. Throughout the entire legal process, victim-centered justice must be ensured. This means keeping the victim safe throughout, with their dignity and privacy prioritised.

Children have the right to protection from sexual exploitation and abuse under Article 34 of the Convention on the Rights of the Child (United Nations, 1989). In addition, the CRC clarified this obligation in the digital environment. Sexual abuse online is a global problem; between 2019 and 2023, there was an increase of 87% in reports of child sexual exploitation and abuse material (WeProtect Global Alliance, 2023). Within those reports were over 61.8 million files (National Center for Missing & Exploited Children, 2025); each of these numbers represents a child. Unlike many crimes, the distribution of CSAM can involve many countries. For example, the material could have been created or obtained in one country, shared using a service based in another country, and sent to many different countries. These discrepancies create jurisdictional friction during cross-border operations as the laws can differ, evidence may be hard to find, and the ability to enforce laws can be low. Not only are children being targeted by strangers online, but according to the UNICEF report (2026), “Through Children’s Eyes: How Digital Technologies Enable Child Sexual Abuse”, approximately 20 million children between the ages 12-17 in 21 countries experienced some form of sexual exploitation/abuse using technology over 1 year. It also shows that mainstream social media and private messaging features can be used to enable abuse (UNICEF, 2026a). This evidence underscores the need to remove illegal material while strengthening

national investigative and legal mechanisms, while also ensuring countries are preventing children from being exploited, investigating crimes, charging those responsible, and providing long-term support to victims.

Because UNICEF is not a law enforcement body, it does not hold the legal authority to enforce domestic criminal penalties. Delegates can create recommendations in the committee to encourage states to make uniform laws, invest in child protection systems, work together, and ensure technology companies and investigators have protection.

After reading this paper, delegates will be able to explain how CSAM is distributed using private messaging services, explain key legal frameworks, and explain what the current situation is in the UN. They will understand why countries and companies disagree and start to create realistic and rights-respecting solutions.

Historical Background

Child Sexual Abuse Material has been an issue for many years before the internet, but advancements in technology have increased the problem. The increase in personal computers, digital cameras, the internet, and file-sharing applications has made it easier to duplicate and share this material across borders during the 1990s. Advancements in social media, mobile technology, and instant messaging applications have significantly expanded digital communication since the early 2000s. This has led to new methods of sharing, contacting, and organizing abuse. For example, the creation of private groups and direct messages. While improvements in encryption have improved privacy for the general public, they have also caused issues with some types of content-based investigations. In recent years, Artificial Intelligence has become a major issue. Images and videos can be produced using artificial intelligence to produce fake sexual material involving children or edit real images. This development complicates efforts establishing who is criminally responsible, identifying victims, determining what level of evidence is needed, and whether current laws are suitable. The exact way AI images are treated can vary depending on the country. Many international agreements have been put into place to help tackle Child Sexual Abuse Material. First, the United Nations adopted the Convention on the Rights of the Child in 1989, codifying protections against sexual exploitation (United Nations, 1989). In 2000, the Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography was adopted. This required

signatory states to make it illegal to exploit children in specific ways (United Nations, 2000). In 2001, the Budapest Convention on Cybercrime was adopted by the Council of Europe. This aims to improve international cooperation to investigate cybercrime, including child sexual abuse material (Council of Europe, 2001). In 2007, the Lanzarote Convention was adopted, and in 2011 the European Union produced Directive 2011/93/EU. Both of these provided more measures to reduce child sexual exploitation, prosecute offenders and protect victims (Council of Europe, 2007; European Parliament & Council of the European Union, 2011). In 2021, the UN Committee on the Rights of the Child published guidance on how children's rights should be applied within the digital environment, highlighting how important it is to protect children while maintaining a balance with their privacy and basic rights (Committee on Rights of the Child, 2021). In 2022, the European Commission proposed new legislation to help tackle child sexual abuse online. This has caused debate around the ability to detect illegal material and how to maintain privacy (European Commission, 2022). In 2024, the UN General Assembly adopted the Convention against Cybercrime to improve international cooperation and electronic evidence (United Nations General Assembly, 2024). More recently, the WeProtect Global Alliance has released a Global Threat Assessment report in 2025, highlighting new issues such as AI-generated material. In 2026, UNICEF produced research showing how common and under-reported technology-facilitated sexual exploitation and abuse still is (WeProtect Global Alliance, 2025; UNICEF, 2026a). This shows how important it is to improve criminal law, improve international cooperation, and ensure that preventing and protecting victims is a priority.

International treaties have provided common rules and requirements to criminalize cooperation; specialised databases and hotlines have also been introduced to help identify victims. For example, INTERPOL has created an International Child Sexual Exploitation database to allow investigators in signatory countries to compare material (INTERPOL, n.d.).

However, international agreements do not always provide consistency. Countries will have different laws, sentencing, and resources to investigate. This can cause issues with identifying perpetrators due to underreporting and difficulty with obtaining electronic evidence. From looking at the history, it can be seen that international agreements are

most effective when there is strong legislation within countries, well-trained investigators, enough funding, full support for survivors, and effective ways to hold people accountable.

Overall, harsh sharing systems, industry reporting, and international cooperation have helped identify abusive material and protect victims. Nevertheless, issues of inconsistent reporting, differing laws, and privacy have hindered progress. Effective solutions should be focused around increasing sentencing but also improving detection, cooperation and the chance of catching offenders.

The Situation Today

There is a global issue with the distribution of Child Sexual Abuse Material (CSAM). In 2025, there were 21.3 million reports of CSAM made to NCMEC and over 311,000 confirmed reports made to the Internet Watch Foundation (NCMEC, 2026b; IWF, 2026). An estimated 20 million children between the ages of 12 and 17 across 21 countries were affected by technology-facilitated sexual exploitation or abuse within a single year; on the other hand, less than 1% of these were reported to authorities (UNICEF, 2026a). New threats have emerged in the form of AI-generated abuse materials, grooming, and sextortion. There have been recent negotiations within the European Union to increase criminal penalties for these crimes; however, there are still disagreements regarding the detection of content in private messages. This shows a clear need for greater international collaboration and ensuring the protection of children while maintaining their privacy and cybersecurity.

Criminalizing the distribution of CSAM is no longer a debate, as most states recognize this as a serious offence. That said, there are still disagreements regarding how to detect and investigate these crimes in private messaging apps. There are also debates regarding what appropriate punishments should be for these crimes, what responsibilities technology companies have, and how to deal with newer threats such as AI-generated CSAM.

Several structural factors impede international consensus. First and foremost, there are differing criminal laws and penalties in each country. This can cause issues for cases internationally. Furthermore, whilst end-to-end encryption ensures the privacy and cybersecurity of individuals, it can cause issues with detecting CSAM. Moreover, due to

different legal systems internationally, it can cause issues in investigating crimes across borders. Lastly, the development of new technologies such as artificial intelligence is creating new forms of synthetic CSAM, which may not be covered under current laws. Under-reporting can be a problem as children may be afraid to report due to the stigma. This means there needs to be an easy system for children to report, support for victims, and effective ways to remove abusive material.

Europe has created strong laws regarding CSAM. However, there are still disagreements around encryption, privacy, and mandatory detection of content. North America plays a big role in reporting, as the US has a large role in NCMEC. Still, this can cause issues as there are a lot of reports to investigate. Latin America and the Caribbean have issues with limited resources to investigate, lack of digital knowledge, and evidence sharing. Africa is working on creating laws. They have the Malabo Convention from the African Union, yet there is still an inconsistent ability to prosecute and support victims. The Asia-Pacific region has countries that have strong online safety systems, such as Australia. In contrast, there are also countries with few resources to investigate and support. Overall, there are issues with differing laws, resources, and capacity internationally, meaning there needs to be international collaboration, technical support, and funding.

Below are some example scenarios:

A teenager's private image is shared without consent by other minors in a school group chat, raising questions about how criminal penalties should account for the age, intent, and level of responsibility of those involved. National legal frameworks illustrate why proportionality is important. For example, under the United States federal sentencing framework, 18 U.S.C 225A establishes serious penalties for certain distribution offenses, while the U. S. Sentencing Guidelines (2G2.2) allow sentences to reflect aggravating factors such as distribution for financial gain or to minors (U. S. Sentencing Commission, 2026). In contrast, the European Union's Directive 2011/93/EU establishes minimum requirements for criminalizing distribution while leaving implementation to individual member states (European Parliament and Council, 2011). These frameworks highlight the importance of distinguishing organized or commercial distribution from cases involving minors, which may require age-appropriate legal procedures and

consideration of diversion measures. Other scenarios raise additional challenges such as investigating credible reports of CSAM in end-to-end encrypted groups without undermining privacy and cybersecurity, or obtaining evidence when suspects, platforms, and recipients are located in different countries. Together, these cases demonstrate the need for proportionate penalties, effective investigations, and stronger international cooperation.

There is no set answer, yet it encourages delegates to think about fair, collaborative and victim-focused solutions.

Key Stakeholders and Their Positions

Key stakeholders involved in addressing the distribution of child sexual abuse include national governments divided between civil-liberties protections and mandatory platform surveillance, law execution agencies seeking decryption capabilities, and private messaging platforms defending client-side security. Major technology companies include Meta, Google, Microsoft, and Signal, playing an important role in reporting suspected CSAM, improving platform safety, and cooperating with law enforcement. All of them have different priorities and approaches, however many oppose mandatory client-side scanning because it could require examining private communications before they are encrypted, creating security vulnerabilities, increasing the risk of weakening user privacy. The Convention on the Rights of the Child (1989) outlines the fundamental rights children should have and states that states must take steps to protect children from abuse and sexual exploitation. In addition to this, the Optional Protocol on the Sale of children, Child Prostitution and Child Pornography (2000) requires States Parties to commit to criminalising listed offences against children. The Budapest Convention on Cybercrime (2001) also supports criminalising cyber offences and international collaboration on cyber evidence. The Lanzarote Convention (2007) specifically focuses on the prevention of child sexual exploitation, protecting children and prosecuting offenders. Internationally, General Comment No. 25 (2021) explains how children's rights apply in the digital world. This provides a reminder that children should be

protected and their privacy ensured online. The UN Convention against cybercrime (2024) looks to improve international collaboration and the sharing of cyber evidence. This includes specific offences relating to CSAM. It will come into effect 90 days after the 40th ratification. There are many more tools, including EU Directive 2011/93/EU, the United Kingdom Online Safety Act (2023), the United States Report Act (2024), the Australian Online Safety Act (2021), and the Malabo Convention (2014) from the African Union. These focus on criminalizing certain actions, holding platforms responsible, ensuring online safety, and improving cybersecurity. There have been attempts within the European Union to improve detection, reporting, and removal of CSAM. However, there is still disagreement about encryption, privacy, and detection technologies. Organisations such as INTERPOL, NCMEC, and the Internet Watch Foundation (IWF) provide help in investigating by using international databases, reporting mechanisms, and hash sharing. Initiatives including WeProtect and victim-focused services such as Take it Down help to improve prevention and protection of children. These tools have helped to improve international collaboration and set international standards. However, there are still issues with variation in legislation and punishments, lack of resources for investigation, low reporting rates, and difficulty collecting evidence internationally. Additional improvements are needed to ensure international consistency, appropriate sentencing, tackle AI-generated CSAM, and address offences involving children. Reforms are necessary to improve collaboration between countries and hold technology companies responsible. Any improvements must ensure that privacy, fair process, cybersecurity, and fundamental children's rights are considered.

Past Attempts and Existing Frameworks

Internationally, multiple legal frameworks are in place to combat CSAM. These include the Convention on the Rights of the Child (1989), Optional Protocol (2000), Budapest Convention (2001), and General Comment No.25 (2021). This ensures countries are accountable for protecting children, prosecuting specific crimes, supporting victims and improving international cooperation. Existing regional frameworks, such as the EU Directive 2011/93/EU, the UK Online Safety Act, the USA REPORT Act, the Australia Online Safety Act and the African Union Malabo Convention. The UN Convention

against Cybercrime (2024), has been adopted to help improve international cooperation and sharing of evidence. INTERPOL has an international database which can help with investigations. They also have hotlines, hash sharing and image removal. At the same time, there are challenges to implementing these policies due to differences in laws between countries, different sentences given, and a lack of resources for investigations and reporting. Within the European Union there have been disputes regarding detection technology, encryption, privacy and proportionality. More needs to be done to tackle new issues such as AI generated CSAM, holding platforms accountable, proportionate and child sensitive sentences, improving international cooperation and ensuring sustainable funding for investigators and survivor support. Policies need to be transparent, fair and protect people's privacy. They also need to be regularly reviewed to ensure they are actually reducing harm.

Challenges and Complications

There are many issues that countries face when trying to develop effective strategies regarding CSAM. There are several differences within each country when looking at their laws relating to CSAM. This can be because of issues with differing opinions between states on how to define crimes, what age to set boundaries at, sentencing guidelines and how to deal with AI generated materials. Some countries will favour strict criminal sentencing and mandating platforms to report whilst others will favour protection of privacy, encryption, national sovereignty and civil liberties. This can cause delays when trying to come to an agreement internationally, such as the European Union currently has when discussing online detection methods. Sentencing should be proportionate to the severity of the crime committed, age of the offender, their intention and surrounding circumstances. The person who is distributing for profit and/or repeat offenders should not be treated the same as someone young who is distributing through peer to peer. There are also issues with privacy and encryption. While it can help with investigations to have access to the data, reducing encryption or having to scan mass amounts of private messages can put users at risk and affect their basic rights. Perceptual hashing technologies, such as PhotoDNA, compare digital fingerprints against databases of known abusive material. While this helps identify previously

reported content, it may not detect new or significantly altered material. Automated systems can also cause issues with false positives. There are also limited resources to enforce these laws, especially in developing countries. Specialist investigators, digital forensics tools, safe storage for evidence and support for survivors may not be available. Evidence, suspects and technology companies may be in different countries which can cause issues when investigating. Laws may differ between locations causing delays when accessing vital information. There can also be issues with culture and society causing stigma. Children may feel scared of being punished if they ask for help. In order to have an effective international response, clear guidelines need to be in place, proportionate sentencing, increased collaboration, technical support, accurate reporting, and child-focused support. Member states must build effective responses while also keeping privacy, fair process, cybersecurity and basic rights in mind.

The Committee's Role and Powers

The UNICEF committee has a mandate to advocate for children's rights. While UNICEF cannot introduce national criminal legislation or enforce sentences, the committee can draft recommendations for minimum standards for justice; delegates may recommend in the draft resolution that member states implement minimum standards focused on national legislation, appropriate punishments, specialist training, international partnership, anonymous reporting systems, supporting survivors, and responsible platforms. The committee can also recommend that member states establish protections regarding privacy, procedural fairness, and technical support. Delegates can recommend partnerships with UNODC for criminal justice, OHCHR and the Committee on the Rights of the Child for human rights, ITU for online safety and INTERPOL for international investigations. The final resolution will have a series of preambulatory clauses to provide context to the issue and recommendations. The suggestions will propose actions, who should be responsible for those actions, and how they should be delivered. All recommendations must fit within UNICEF’s advisory role, accurately reflect the nation’s policies, respect differing opinions and most importantly ensure children’s safety as well as respect and rights are prioritised.

Guiding Questions for Debate

Delegates should research their country's legal framework, international commitments, technology policies, and child-protection priorities before addressing these questions.

1. Should countries establish international minimum standards for criminal penalties for distributing CSAM, and how can these standards respect national legal systems?
2. How should sentencing distinguish between different forms of distribution, including repeat offending, commercial exploitation, and organized criminal activity?
3. What safeguards can ensure the stronger criminal penalties deter serious offenses without producing disproportionate punishment or undermining due process?
4. How can governments improve investigations involving end-to-end encrypted messaging while protecting privacy and cybersecurity for legitimate users?
5. Should technology companies face additional legal obligations when CSAM is distributed through their services, and how should responsibility be determined?
6. How can countries improve cross-border evidence-sharing and victim identification while respecting human rights and national legal requirements?
7. What legislative changes may be needed to address AI-generated CSAM, and how can these laws remain clear and enforceable as technology develops?
8. How can governments increase reporting by children and families without exposing victims to retaliation, stigma, or unnecessary disclosure of personal information?
9. What financial and technical assistance should higher-capacity countries and international organizations provide to states that lack specialized investigative resources?
10. How should the international community measure whether stronger penalties and related policies actually reduce distribution, improve prosecutions, and protect children?

11. What standards should govern the use of automated detection technologies including safeguards against false positives, misuse and unauthorized access to private information?
12. What international measures can help countries cooperate in investigating and prosecuting individuals who distribute CSAM through private messaging platforms across national borders?

Conclusion and Call to Action

The distribution of Child Sexual Abuse Material (CSAM), via private messaging apps is an international issue. Thanks to advancements in digital technology, this has increased the speed at which abusive content circulates. Additionally, investigating cases across borders has become more challenging. There are millions of reports every year, alongside the increase of online grooming and sextortion. In addition, new technologies such as Artificial Intelligence are creating more CSAM. This demonstrates how important international cooperation is to tackle this issue (NCMEC, 2026b; Digital Watch Observatory, 2026; UNICEF, 2026). International treaties, legislation and reporting systems have been put into place to help address this. However, there are still major issues with lack of consistent legislation, low reporting rates, lack of investigative resources and differing opinions around privacy and end-to-end encryption. With international and regional regulations increasing, delegates can work together to create better international cooperation. This will ensure child protection is improved, whilst not affecting basic human rights. Implementing harsher punishments within the criminal justice system can help to hold people accountable. Nonetheless, to truly keep children safe, governments need to invest in preventative measures, making it easy for victims to report, supporting victims, promoting responsible use of technology and providing specialist training. Considerations should be taken into account such as the age of the offender, their intent and involvement to ensure fair processes are in place and to protect privacy and cyber security. UNICEF is an important organization to consider when looking at this issue from a child's rights perspective. Delegates should take existing international agreements into consideration, taking into account the differing situations in each country. Practical recommendations can be created to ensure there is effective criminal justice, alongside preventative measures, international cooperation

and victim protection. The aim of this is to create a digital world which protects children from exploitation. All recommendations should be considered with the question in mind: Will this keep children safe while protecting their rights, dignity, and privacy?

References

Brown, S. (n.d.). *Child sexual abuse by adults in online contexts*. Centre of Expertise on Child Sexual Abuse. Retrieved November 5, 2026, from https://www.csacentre.org.uk/research-resources/key-messages/key-messages-from-research-on-child-sexual-abuse-by-adults-in-online-contexts/

Campbell, J., Kravarik, J., & Clark, J. F. (n.d.). *Child Sexual Abuse Material*. Department of Justice. Retrieved November 5, 2026, from https://www.justice.gov/d9/2023-06/child_sexual_abuse_material_2.pdf

Child sexual abuse material and end-to-end encryption on social media platforms: An overview. (n.d.). Australian Institute of Criminology. Retrieved November 5, 2026, from https://www.aic.gov.au/sites/default/files/2022-07/ti653_csam_and_end-to-end_encryption_on_social_media_platforms.pdf

Convention on the Rights of the Child. (n.d.). UNICEF. Retrieved November 5, 2026, from https://www.unicef.org/child-rights-convention

Global Threat Assessment 2025. (n.d.). WeProtect Global Alliance. Retrieved November 5, 2026, from https://www.weprotect.org/global-threat-assessment-25/

How Does CSAM Get Distributed? (n.d.). RAINN. Retrieved November 5, 2026, from https://rainn.org/get-the-facts-about-csam-child-sexual-abuse-material/how-does-csam-get-distributed/

International Child Sexual Exploitation database - Crimes. (n.d.). Interpol. Retrieved November 5, 2026, from https://www.interpol.int/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database

Key Definitions. (n.d.). Homeland Security. Retrieved November 5, 2026, from https://www.dhs.gov/know2protect/key-definitions

Latest online child sexual abuse and exploitation data. (n.d.). Safer by Thorn. Retrieved November 5, 2026, from https://safer.io/resources/csam-problem-of-epidemic-proportions/

Missing the mark? Identifying child sexual abuse material forum structure and key-players based on public replies and private messaging networks | Humanities and Social Sciences Communications. (n.d.). Nature. Retrieved November 5, 2026, from https://www.nature.com/articles/s41599-024-03954-x

Nuevo estudio: Uno de cada ocho adolescentes en México sufrió explotación o abuso sexual en línea. (n.d.). UNICEF. Retrieved November 5, 2026, from https://www.unicef.org/mexico/comunicados-prensa/nuevo-estudio-uno-de-cada-ocho-adolescentes-en-m%C3%A9xico-sufri%C3%B3-explotaci%C3%B3n-o-abuso

1 in 5 children across 21 countries have experienced tech-facilitated sexual exploitation and abuse – UNICEF. (n.d.). UNICEF. Retrieved November 5, 2026, from https://www.unicef.org/press-releases/1-5-children-across-21-countries-have-experienced-tech-facilitated-sexual

Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography. (n.d.). ohchr. Retrieved November 5, 2026, from https://www.ohchr.org/en/instruments-mechanisms/instruments/optional-protocol-convention-rights-child-sale-children-child

Protecting children from sexual abuse - Migration and Home Affairs. (n.d.). Migration and Home Affairs. Retrieved November 5, 2026, from https://home-affairs.ec.europa.eu/policies/internal-security/protecting-children-sexual-abuse_en

Resources & Research: Reviewing Child Sexual Abuse Material Reporting Functions on Popular Platforms. (n.d.). Canadian Centre for Child Protection. Retrieved November 5, 2026, from https://protectchildren.ca/en/resources-research/csam-reporting-platforms/

UNTC. (n.d.). UNTC. Retrieved November 5, 2026, from https://treaties.un.org/Pages/ViewDetails.aspx?chapter=18&mtdsg_no=XVIII-16&src=TREATY

What we do. (n.d.). UNICEF. Retrieved November 5, 2026, from https://www.unicef.org/what-we-do