Chapter 2

The issue & our solution to online CSAM

Any sexual activity with a minor constitutes child sexual abuse because a child cannot give consent to sex. This includes physical acts, whether through force, coercion, grooming, or implied force. This applies to sexual activity between an adult and a minor and might also include sexual activity between a significantly older and a younger child. Verbal acts, such as sexual harassment or trying to show a child pornography, and non-touching acts, such as voyeurism or an adult showing their own genitals to a child also constitute sexual abuse. This applies both in person and online. Sexual abuse has long-lasting and detrimental physical, psychological, and emotional consequences for the child.

Child Sexual Abuse Material (CSAM) refers to the recording or depiction of child sexual abuse and constitutes a secondary form of abuse. We use this acronym in communication, and it is a well-used term globally, but it must never be forgotten that these four letters refer to recorded imagery of the sexual abuse of children, where there are real victims, and that it is a serious crime. The physical element may stop at some point, but the psychological damage caused to victims is repeated every time that CSAM is viewed or shared. To know that this abuse is still on the internet for anyone to view can make daily tasks challenging for victims even many years after their rescue, knowing that someone in the supermarket or doctor's surgery might have viewed their abuse.

2.1 Background issues on CSAM

Our lives have been markedly transformed by the advent of the internet. There are 2.2 billion people globally under the age of 18, making them society's biggest group, and the most vulnerable to online harm (UNICEF, 2020). Children in developed countries live in the digital world every day, for school and homework, for shopping, gaming, maintaining, and making friendships and more. Children in developing countries are less likely to have 'grown up online' in the same way, but around the world a child goes online for the first time every half second (UNICEF, 2020), so, children everywhere need help to understand the risks of the online world and to build the resilience to cope with these risks.

The internet and digital technologies have transformed our world and the way we interact. We have cheaper, faster, more diverse, more accessible, more secure forms of information access, information sharing and communication than ever before. The benefits of this are immense and overwhelmingly positive. However, among the challenges presented by our online world are the production, distribution and possession and viewing of the online sexual exploitation and abuse of

children. Sadly, some of the key benefits of the online world, including privacy, security, and freedom of access to information, also present challenges for the online protection of children, including prevention and response strategies[2].

2.2 The numbers

According to the World Health Organisation (WHO), 200 million children are sexually abused every year (Lu, J 2019). This is an extreme figure that we cannot look away from. Individual countries are contributing to this figure and behind this figure are the victims. To see how prepared your country is to deal with the threat of child sexual abuse and exploitation, you can look at the Economist Intelligence Unit's study and tool, Out of the Shadows (The Economist Intelligence Unit, 2019). The study reviewed 60 countries using a benchmarking index that provides invaluable insight by examining how countries are responding to the threat of sexual violence against children, by reviewing the environment and legal framework set up to protect children, the government's commitment, industry engagement and civil society. Child sexual abuse and child exploitation are not new issues, and as we increasingly migrate to a virtual, as well as physical society, we see a parallel rise in the amount of CSAM recorded and distributed. Through ICCAM, INHOPE's hotlines feed INTERPOL's International Child Sexual Exploitation database (ICSE), which holds more than 1.5 million images and videos, collectively recording the abuse of more than 19,400 victims worldwide (INTERPOL 2019). ICSE is a powerful investigative tool made available by INTERPOL to certified, specialised investigators in its global network to access and collaborate on victim identification data.

In 2020, INHOPE hotlines across the world exchanged more than one million URLs of CSAM —1.038.268 to be precise. 48% of these URLs were normal websites, 24% image hosting sites, 13% file hosting sites and the remaining were forums, banner sites, link sites and social media. 60% of the reported material was previously known content, which shows that CSAM is repeatedly circulated on the internet, and collaboration between hotlines worldwide is crucial to stop the redistribution of this material.

[2] Click here to read an article which addresses some of the challenges of online child protection, prevention and privacy, social media, resilience (Quayle, 2020)

2.3 WePROTECT Global Alliance's Model National Response

While the challenge is real, there is also hope. We see more and more actors committing themselves to a collective response, and we have ever more tools at our disposal to respond to this epidemic. Increasingly, partnerships and collaboration across the technology industry, governments, global institutions, and NGOs are helping to build efficient, effective, and fair response mechanisms that assist the work of police and industry in eradicating and combatting online child sexual exploitation and abuse. One such tool that provides a country with a framework for the development of a national strategy is the WePROTECT Global Alliance's Model National Response. At a Summit in 2015, governments, NGOs and other global and national institutions agreed to establish and deliver a coordinated national response to online child sexual exploitation, guided by the WePROTECT Global Alliance Model National Response. This resource is hugely helpful for anyone wishing to help their country take national ownership of the issue of online CSAM.

The Model National Response clarifies the role of INHOPE and the network of hotlines as well as all the other key stakeholders' roles, and the capabilities and competencies that must be developed and implemented. As we start to work together on the creation of your hotline, you will see that we bring all national stakeholders together. This is to raise awareness of the work of the hotline but also as a way of ensuring that all aspects of online CSAM as defined in the Model National Response are identified, raised, and tackled. We will work with you to create a child online safety prevention, protection and care strategy in your country if you do not yet have one.

You can verify if your country is already a signatory to the WePROTECT Global Alliance's Model National Response by clicking here. If it is, you are off to a solid start, and you will be able to find out what plans and measures are in place to tackle online CSAM.

2.4 Defining CSAM nationally: Getting it right from the start

As mentioned above, child sexual abuse material (CSAM) is the permanent recording of the sexual abuse or exploitation of a child and depicts actual crime scenes. Real children are being abused on camera and film and there is nothing virtual about their suffering. It is crucial that we all call this crime exactly what it is and ensure that others do as well.

Art. 2(c) of the Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution, and Child Pornography, adopted and opened for signature, ratification and accession by General Assembly Resolution A/RES/54/263 of 25 May 2000 entered into force on 18 January 2002. It describes **child pornography** as "any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or representation of the sexual parts of a child, the dominant characteristics of which is depiction for a sexual purpose."

However, while the term 'child pornography' is still widely used, especially in the context of legislation, INHOPE and its partners refer to Child Sexual Abuse Material to describe the phenomenon. This term more accurately reflects the seriousness of the nature of the content and challenges any notion that such acts might be carried out with the consent of the child.

You can read more about terminology about this crime type here in the Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (Luxembourg Guidelines, created by ECPAT International) and also in INTERPOL's Guidance on Appropriate Terminology here.

2.5 Other forms of online child sexual exploitation and abuse

CSAM is one category of a wider panorama of online child sexual exploitation and abuse. Existing and major challenges in this area include the following but this is not an exhaustive list:

- Online grooming of children.
- Sexting.
- Sexual extortion.
- Live streaming of Child Sexual Abuse.
- Consuming Child Sexual Abuse Material.
- Deepfakes.

2.6 Issue - Who are the perpetrators of child sexual abuse?

The perpetrators of online CSAM or offline child sexual abuse are most commonly known to the child, either within the family, or in a position of authority outside the family but with regular access to the child. They are of every race and ethnicity, from every walk of life and profession, and although more commonly male, can be male or female.

There are three commonly recognised categories of abusers:

- Preferential Offenders: who are motivated by sexual interests exclusively felt for children (i.e., paedophiles/hebephiles).
- Commercial Offenders: who facilitate child sexual abuse simply for their own financial gain.
- Situational Offenders: who take advantage of opportunities to engage with CSAM and minors, but do not have a true or exclusive sexual preference for children.

2.7 Solution - The removal of CSAM: Notice and Takedown

The INHOPE network of hotlines cooperates daily to facilitate the rapid removal of CSAM from public access. This is a process commonly referred to as 'Notice and Takedown.' You can learn more about the process by clicking here.

A Notice and Takedown order is the procedure INHOPE has in place whereby a hosting provider or search engine is asked to immediately remove or disable access to online CSAM information hosted on their services. INHOPE member hotlines send Notice and Takedown orders to hosting providers either when:

1. A member of the public sends them a URL containing illegal images and videos depicting child sexual abuse and exploitation which is hosted in their own country.
2. Another INHOPE member sends through ICCAM suspected CSAM hosted in your country.

Once you are a member of INHOPE, you are able to receive reports from other hotlines around the world, of suspected CSAM that is hosted in your country. If it is CSAM according to your national law, you will send a Notice and Takedown order to the national hosting provider in your country for removal. Once you have traced the URL and know which country is hosting the material, you will insert the URL into ICCAM for the hosting country's hotline to send the Notice and Takedown order to the HP. Most hosting providers respond by swiftly removing the content. This is one of the areas where the importance of swift, smooth, and clear communication with your national hosting providers is key for rapid removal of the content.

2.8 A note on prevention

While the purpose of this document is not to discuss prevention measures as we talk about the issue and how a hotline is part of the solution, there are many prevention measures that exist and are being developed around the world. We encourage organisations applying to become INHOPE hotlines to collaborate with colleagues and stakeholders in their countries to contribute to the prevention and protection initiatives in their countries as much as possible. See INHOPE's Prevention Initiatives Report here for some examples of how some of our hotlines work with prevention strategies and organisations in their countries today. INHOPE hotlines report that significant numbers of children are being groomed via the chat function of online games and social media. Never before has it been easier for perpetrators to make contact with children, share images including those of abuse, normalise the behaviour of their criminal peers, hide their identity and profits – and inspire each other to commit further. Hotlines address the removal of the material that exists as a consequence of these crimes.

Those that produce, record, distribute or consume online CSAM will be held to account for their crimes as a result of a report to an INHOPE hotline. Each form of online child exploitation or abuse requires a specific response protocol, as well as a customised prevention and awareness-raising strategy.

2.9 A note on blocking as a preventive measure

INHOPE does not encourage blocking, rather removing material 'at source,' so that wherever you are in the world the CSAM is inaccessible.

Blocking material in your country means that only the citizens in your country are unable to view this illegal material online, but it remains visible for the rest of the world. Therefore, INHOPE's preferred approach is to remove the material from the source so it is no longer accessible on the internet for anyone anywhere in the world. However, some hotlines contribute to the creation of a national URL block list. This does prevent access in the country in which it was blocked, and blocking can prevent revictimisation albeit only in the short-term. A block list could be a list of URLs confirmed to contain CSAM that meet the national definition of illegal in the country of the hotline.

The use of a block list may be defined by law or on a voluntary basis by the private sector, and the dynamics of access blocking vary from country to country. Useful as a preventive and interim measure, access blocking prevents a user from accessing illegal content while it is being removed at source. For countries without a national block list, you can visit the INTERPOL website to learn more about INTERPOL's International Worst of List here.

The IWOL list is a combination of prevention mechanisms on the web by various actors to deter the commercial exploitation of children via websites. In the case that the website content matches the restrictive IWOL criteria, it can be included in the IWOL list in cooperation with the relevant hosting provider and the national authorities. The domain is then added into a filter to interdict the access to the contained material to the end user. This is available for public and private sector implementation at country level.