SUMMARY PAPER ON

ONLINE CHILD SEXUAL EXPLOITATION

ECPAT International is a global network of civil society organisations working together to end the sexual exploitation of children (SEC). ECPAT comprises member organisations in over 100 countries who generate knowledge, raise awareness, and advocate to protect children from all forms of sexual exploitation.

Key manifestations of sexual exploitation of children (SEC) include the exploitation of children in prostitution, the sale and trafficking of children for sexual purposes, online child sexual exploitation (OCSE), the sexual exploitation of children in travel and tourism (SECTT) and some forms of child, early and forced marriages (CEFM). None of these contexts or manifestations are isolated, and any discussion of one must be a discussion of SEC altogether.

Notably, these contexts and manifestations of SEC are becoming increasingly complex and interlinked as a result of drivers like greater mobility of people, evolving digital technology and rapidly expanding access to communications. Now more than ever, the lines between different manifestations of SEC are blurred and children may be victimised in multiple ways.

The ECPAT Summary Papers explore each of these five manifestations but should be considered a set addressing this complex problem. This Summary Paper focuses attention on OCSE.

The Internet is a part of children's lives. Information and Communication Technologies (ICT) are now as important to the education and social development of children and young people as they are to the overall global economy. According to research, children and adolescents under 18 account for an estimated one in three Internet users around the world[1] and global data indicates that children's usage is increasing – both in terms of the number of children with access, and their time spent online.[2] While there is still disparity in access to new technologies between and within countries in the developed and developing world, technology now mediates almost all human activities in some way. Our lives exist on a continuum that includes online and offline domains simultaneously. It can therefore be argued that children are living in a digital world where on/offline

1 Livingstone, S., Carr, J. and Byrne, J. (2016). One in three: Internet governance and children's rights. *Innocenti Discussion Paper,* No.2016-01, UNICEF Office of Research, Florence. 7.

2 UNICEF Office of Research- Innocenti. (2019, November). Global kids online. Comparative report. UNICEF Office of Research, Innocenti: Florence, Italy. 8.

distinctions no longer represent separate social spaces.[3] This is certainly the case when considering child sexual abuse and exploitation too. Both online[4] and offline,[5,6] evidence indicates that most child sexual abuse and exploitation is committed by adults in the child's circle of trust.[7]

As the world increasingly connects through technology, an array of risks is also present. Broader Internet penetration and an expanding use of mobile devices enables the circumstances for offenders to misuse technology with an aim to contact, groom and abuse children.[8] Additionally, the easy availability of encrypted messaging platforms, peer to peer networks, and easy access to the 'Darknet' make it easier for perpetrators to connect, cooperate, evade identification and share child sexual abuse and exploitation material (CSAM/CSEM). [9,10,11]

The Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (the 'Luxembourg Guidelines') define online child sexual exploitation (OCSE) as: '*all acts of a sexually exploitative nature carried out against a child that have, at some stage, a connection to the online environment. It includes any use of ICT that results in sexual exploitation or causes a child to be sexually exploited or that results in or causes images or other material documenting such sexual exploitation to be produced, bought, sold, possessed, distributed, or transmitted.*' This definition emphasises that OCSE is not, in and by itself, a distinct type of sexual exploitation of children (SEC). As an umbrella term, it captures all SEC-related criminal conducts and manifestations that have an online or technology related component at some point.

Until the beginning of the 2000's, the problem of OCSE was mostly confined to the production, possession and distribution online of CSAM/CSEM. However, the dynamic nature of ICTs has expanded the notion of Internet facilitated child sexual exploitation to include an evolving range of practices such as live streaming of child sexual abuse,[12] 'online grooming'[13] and online sexual extortion and coercion[14] among others (see box for definitions).

LIVE STREAMING

"Live online child sexual abuse often represents a dual abuse of the child. She/he is coerced to participate in sexual activities, alone or with other persons—an act that already constitutes sexual abuse. The sexual activity is, at the same time, transmitted live through ICT and watched by others remotely.[…] Live online child sexual abuse is often transmitted to viewers through 'streaming' over the Internet."

ONLINE GROOMING

"In the context of child sexual exploitation and sexual abuse, 'grooming' is the short name for the solicitation of children for sexual purposes. 'Grooming/online grooming' refers to the process of establishing/building a relationship with a child either in person or through the use of the Internet or other digital technologies to facilitate either online or offline sexual contact with that person."

3 May-Chahal, C. et al. (2014). Safeguarding cyborg childhoods: Incorporating the on/offline behaviour of children into everyday social work practices. *British Journal of Social Work,* 44 (3): 596-614.
4 ECPAT International and INTERPOL. (2018). Towards a global indicator on unidentified victims of child sexual exploitation – Technical Report. 22.
5 Finkelhor. D. & Shattuck, A. (2012, May). Characteristics of crimes against juveniles. New Hampshire, USA: Crimes against Children Research Centre, University of New Hampshire. 5.
6 US Department of Health & Human Services, Administration for Children and Families, Administration on Children, Youth and Families, Children's Bureau. (2020). Child Maltreatment 2018. USA: Children's Bureau. 57.
7 Lanzarote Committee. (2015). Protection of children against sexual abuse in the circle of trust: The strategies. Strasbourg: Council of Europe. 3.
8 EUROPOL. (2018). Internet Organized Crime Threat Assessment 2018. 30-31.
9 *"Child sexual exploitation material' can be used to encompass all sexualised material depicting children, including 'child sexual abuse material' which refers specifically to material depicting acts of sexual abuse and/or focusing on the genitalia of the child. The distinction between CSEM and CSAM is generally one of legal status, although detailed definitions and indeed use of these key terms varies between countries and languages."* ECPAT International and INTERPOL. (2018). Towards a global indicator on unidentified victims of child sexual exploitation – Technical Report. xii.
10 United Nations Office on Drugs and Crimes. (2015). Study on the effects of new Information Technologies on the abuse and exploitation of children, Vienna: United Nations Office. 15-17.
11 ECPAT International. (2018). Trends in online child sexual abuse material. Bangkok: ECPAT International. 32.
12 Interagency Working Group on Sexual Exploitation of Children. (2016). Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse. 46-47.
13 *Ibid.,* 51.
14 *Ibid.,* 52.

ONLINE SEXUAL EXTORTION AND COERCION

"Sexual extortion, also called 'sextortion', is the blackmailing of a person with the help of self-generated images of that person in order to extort sexual favours, money, or other benefits from her/him under the threat of sharing the material beyond the consent of the depicted person (e.g. posting images on social media)."

Moreover, ICTs are now increasingly being used by a range of exploiters. This includes those who offend children online; as well as offenders who seek offline contact with children using ICTs to connect with and groom them.[15] The Internet also allows anonymous global connections between people and makes it easier for offenders to make connections, share information and coordinate their crimes. Additional to these are facilitators – who may not consume materials themselves – but who make money by misusing technology to perpetuate sexual exploitation of children.[16]

Governments and the international community have increasingly acknowledged the threat of OCSE. Protective legislation and preventive measures have been adopted in many countries and several initiatives have been launched to tackle this crime at all levels. A strong example is the WePROTECT Global Alliance and its Model National Response, which provides a policy framework to develop cross-sector capabilities to end OCSE.

Although at global, regional and national levels, political commitment has improved over the last decade, there are ever-increasing reports of children all over the world being sexually abused and exploited where technology is involved in the process. The overall volume of CSAM/CSEM circulating online continues to grow at unprecedented rates[17] and, anecdotally, law enforcement indicates that the collections of CSAM/CSEM that offenders are caught with are now routinely very large, and with an increasing share of videos versus still pictures. Multiple sources indicate that the volume of reported OCSE cases, and in particular reported CSAM, is increasing. Online reporting mechanisms known as hotlines are mandated to assess online content referred to them by Internet users and/or ICT companies to determine its nature and legality. Some of these hotlines, such as the Internet Watch Foundation,[18] are now increasingly proactively detecting CSAM online by scanning the Internet. Data from the Internet Watch Foundation 2019 Annual Report, show a staggering increase in reports since the foundation started proactively searching for CSAM. Indeed, in 2013, the last year prior to the Internet Watch Foundation introducing proactive searches, 13,182 webpages containing CSAM were identified.[19] This is compared to 132,672 in 2019[20] (a 1006% increase). Another example of proactive detection is provided by Cybertip Canada's Project Arachnid, which identifies CSAM by systematically browsing the net using web crawlers. The US-based National Center for Missing and Exploited Children, which operates the reporting mechanism CyberTipline, reported in 2019 that it received over 16.9 million reports of suspected child sexual exploitation, out of which only 150,667 (less than 1%) came from the public and the rest from electronic communications providers, the majority from Facebook owned platforms. It is worth noting that since 2008, all US based electronic communications providers are legally required to report CSAM to the National Center for Missing and Exploited Children.[21]

The increases in reported and detected CSAM can partially be explained by the numerous methods now available to report, and by entities dedicated to proactive detection as described above. But the sheer scale of the data does also imply that incidences of these crimes are likely increasing as well.

During the COVID-19 pandemic in 2020, sources such as law enforcement agencies, child helplines and online reporting mechanisms indicated increased reporting of a range of online related

15 Grocki, S. (2016). Sexual exploitation of children in tourism and online.
16 Interagency Working Group on Sexual Exploitation of Children. (2016). Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse. Bangkok: ECPAT International. 89.
17 ECPAT International and INTERPOL. (2018). Towards a global indicator on unidentified victims of child sexual exploitation – Technical Report. 20.
18 Internet Watch Foundation. (2020, April). The Why. The How. The Who. And the Results. The Internet Watch Foundation Annual Report 2019.
19 Internet Watch Foundation. (2013). Internet Watch Foundation Annual and Charity Report 2013. Cambridge, UK: Internet Watch Foundation. 6.
20 Internet Watch Foundation. (2020, April). The Why. The How. The Who. And the Results. The Internet Watch Foundation Annual Report 2019. 46.
21 18 U.S. Code § 2258A. Reporting requirements of providers.

child sexual abuse and exploitation.[22] This may be a result of children and offenders coping with movement restrictions and being online more often. It could also be that during movement restrictions, global attention turned to our online lives and more vigilance led to more concerns being raised.[23] Warnings of an expected rise in abuse and exploitation occurring in home environments were voiced by many agencies, including EUROPOL.[24]

In October 2020, EUROPOL highlighted in the 2020 Internet Organised Crime Threat Assessment that the amount of CSAM detected continued to increase, exacerbated by the COVID-19 pandemic. Further, the report explained how the live streaming of child sexual abuse increased during the pandemic, as travel restrictions prevented offenders from physically abusing children.

Despite increased attention on OCSE during this period, in a publication released in September 2020, INTERPOL indicated that the COVID-19 pandemic in fact had resulted in fewer reports reaching police, difficulties in moving forward with existing investigations and reduced use of the global International Child Sexual Exploitation (ICSE) database due to movement restrictions and other priorities faced by law enforcement personnel.[25]

Law enforcement, ICT companies, reporting platforms and child protection agencies find themselves outpaced as they try to combat an ever-changing and ever-growing threat from perpetrators.[26] But whereas the platforms and methods used by offenders and criminal networks may change, the impact of sexual abuse and exploitation on child victims does not. OCSE has devastating, far-reaching and long-lasting effects on children and young people.[27] An effective, coordinated and comprehensive national and international response to all forms of online child sexual abuse and exploitation is, therefore, of the utmost importance.

Ending OCSE has been among ECPAT's ambitious goals since the second half of the 1990s when the organisation commissioned a thematic paper on 'child pornography,' (note that ECPAT now discourages use of this term, using 'child sexual abuse material' or CSAM instead)[28] in preparation for the First World Congress Against the Commercial Sexual Exploitation of Children that took place in Stockholm, Sweden in 1996.[29] This Summary Paper outlines the contemporary issues that ECPAT considers vital to effective prevention and responses to OCSE. It is informed by our leadership on this topic, the global evidence, survivors' advocacy, and seminal expert positions and sources.

22 *See e.g.* Europol. (2020, 19 June). Exploiting isolation: Offenders and victims of online child sexual abuse during the COVID-19 pandemic. National Center for Missing and Exploited Children. (2020, 16 July). COVID-19 and missing & exploited children.
23 INTERPOL. (2020, September). Threats and trends. Child sexual exploitation and abuse. COVID-19 Impact.
24 *See e.g.* EUROPOL. (2020, 19 June). Exploiting Isolation: Offenders and victims of online child sexual abuse during the COVID-19 pandemic. National Center for Missing and Exploited Children. (2020, 16 July). COVID-19 and missing & exploited children.
25 INTERPOL. (2020, September). Threats and trends. Child sexual exploitation and abuse. COVID-19 Impact. 7.
26 ECPAT International. (2018). Trends in online sexual abuse material. 6.
27 Canadian Centre for Child Protection. (2017). Survivors' Survey. Full report 2017. 15.
28 ECPAT now prefers the term 'child sexual exploitation material' or 'child sexual abuse material' instead of 'child pornography' in line with the widely adopted Terminology Guidelines. 39.
29 Healy, M.A. (1996). Child pornography: an international perspective. ECPAT International.

KEY CHALLENGES AND TRENDS

Like all forms of child sexual exploitation, it is difficult to gauge the true scope of OCSE as it is estimated that the majority of cases go unreported. However, integral research continues to shed light on the nature of this crime. A 2018 ECPAT and INTERPOL study conducted an analysis of information recorded for one million items depicting child sexual abuse and exploitation drawn from the ICSE database, hosted by INTERPOL. These one million items are uploaded by and on behalf of member countries as a result of investigations into online child sexual abuse. The analysis showed that where victim gender was recorded, 64.8% of these were girls and 30.5% were boys. In these images, where the abuse depicted boys and very young children, the abuse was likely to be more severe. The research also showed that where the ethnicity of abusers and victims portrayed could be determined, offenders appear to have a preference for victims of the same ethnicity. However, it should be noted that this could be the result of proximity and opportunity when the offender is part of the child's 'circle of trust' – their family or community. It may also be indicative of travelling sex offenders moving domestically or regionally to offend. Another interesting finding relates to the difficulty researchers encountered in categorising sexual materials which had been self-generated (i.e. created by the child). This task was easier with video material than pictures as more information on whether the child may have been extorted or coerced were available in the context of production.

The above findings also aligned with trends observed by law enforcement professionals in an ECPAT 2018 qualitative study. Respondents indicated that they believed that images showing a greater level of sexual violence had increased over time, with more egregious images generally associated with younger children and often produced within a family context. Law enforcement professionals indicated that most of the CSAM they had seen depicted pubescent and pre-pubescent children, while the number of very young children (infants and toddlers) has remained relatively low. With regards to self-generated sexual content, a 2018 NetClean Report corresponds with ECPAT and INTERPOL's analysis, indicating that some of the police officers interviewed reported difficulties in determining whether an image has actually been produced voluntarily or following an exploitative situation, such as grooming or sexual extortion.

In terms of ethnicity, existing evidence tends to suggest that the majority of both victims and offenders are white Caucasians,[30,31] however, this analysis depends on the available data sources which are skewed towards the developed world. For example, the current geographical scope of countries connected to INTERPOL's ICSE database is limited to countries that have signed up.[32] Though limited in numbers, the noted increase of other ethnic groups in recent years deserves further investigation given growing concerns about emerging cases of OCSE in developing countries.[33]

Recent trends in child victims' gender also deserve further analysis. Although girls continue to be victimised more than boys in CSAM production, boys do make up significant proportions. As mentioned earlier, ECPAT and INTERPOL 2018 analysis showed 30.5% of images included boys, and that sexual exploitation materials of boys were also more likely to be severe or involve paraphilic themes and violence. Further, in 2011, 20.1% of images in the UK Child Exploitation and Online Protection Centre database were found to be of boys.[34] INHOPE

30 ECPAT International and INTERPOL. (2018). Towards a global indicator on unidentified victims of child sexual exploitation – Summary Report. 4.
31 NetClean. (2016). NetClean Report 2016. Insight three.
32 ECPAT International and INTERPOL. (2018). Towards a global indicator on unidentified victims of child sexual exploitation – Summary Report. 1.
33 ECPAT International. (2018). Trends in online sexual abuse material. 5.
34 Quayle, E., & Jones, T. (2011). Sexualized images of children on the Internet. Sexual Abuse, 23(1). 7–21.

annual data reported a marked increase in the proportion of boys depicted in reported CSAM from 4.3% in 2017 to 16.8% in 2018.[35]

There is a continuum of abuse and exploitation between the online and offline worlds. The sexual violence we observe in images and videos online is a record of the sexual violence children suffer offline. CSAM produced and shared online are the digital evidence of hands on sexual abuse committed against that child portrayed on the images.

The boundaries between the physical and digital world are blurring, and even the term 'online' can be problematic as it still implies a deliberate discrete act of 'using the Internet' when for many, we are connected throughout our waking hours.[36] While that brings many positives, there are also risks. As lives increasingly become enmeshed with technology and the Internet, this impacts children too – they are online earlier and for greater proportions of their time.[37] More time online does increase potential risks of children encountering offenders, however, exposure to risk does not automatically mean more harm. The growth in social media use, gaming and child focused online spaces creates opportunities for offenders to access and groom children.[38,39]

Moreover, the digital age is challenging and shifting notions of privacy and sexuality, particularly among adolescents.[40] Increasingly, law enforcement are reporting that a growing proportion of CSAM/CSEM comprises of 'self-generated' sexual content.[41] These images may be the result of a grooming process whereby an adult gains the trust of a child online and then convinces them to commit and record sexual acts. These deceived young people are then sometimes coerced into producing and sharing more content in a process known as 'sexual extortion'. However, in many cases young people are consensually making and sharing images with peers (i.e. sexting) that may not have negative repercussions but may also later end-up circulating the web and being acquired by offenders.[42]

The live streaming of child sexual abuse has also become an established reality. Distant live-streaming can be facilitated by family members or other adults known to the child, sometimes also participating in the hands-on abuse performed in front of the camera.[43] Through technology, including international micro-finance transfers and video-streaming tools, offenders can order for specific abuse to be perpetrated, pay for it and view the abuse as it takes place elsewhere. Identified cases have tended to take advantage of economic disparity, with perpetrators from developed countries accessing victims in developing countries, but this is not exclusively the case. This phenomenon is particularly widespread in some countries of Southeast Asia, particularly those where English is widely spoken, but has also been reported in Eastern Europe, South America, Russia and the US.[44, 45]

Another emerging trend that needs to be monitored is the use of entertainment tools based on virtual reality technology to contact children for the purpose of sexual exploitation. Notably, it has been argued that immersive video games incorporating haptic technologies that enable the delivery of sensation to wearers, may attract those with a sexual interest in children. Child sexual abuse through virtual reality technology has already been documented, but its future developments, implications and impact on children are yet to be fully understood.[46]

Similarly, evolving technological innovations present potential ways for perpetrators to exploit children.[47] NetClean's 2019 report notes emerging technologies that may be misused for sexual exploitation of children. Increasing use of cloud storage and peer to peer networks, encryption technology and artificial intelligence are named. Offenders are increasingly avoiding sharing CSAM directly and rather share links to online spaces where the materials can be accessed. The report highlights how encryption is seen as one of the biggest challenges for detecting

35 INHOPE. (2019). Annual Report 2018. 24.
36 Livingstone, S and Stoilova, A. (n.d.). Understanding children online: Theories, concepts, debates.
37 *See e.g.* Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Olafsson, K., Livingstone, S., and Hasebrink, U. (2020). EU Kids Online 2020: Survey results from 29 countries. 77-79.
38 NetClean. (2019). NetClean Report 2019: A report about child sexual abuse crime. 4.
39 INTERPOL. (2020, September). Threats and trends. Child sexual exploitation and abuse. COVID-19 Impact. 12.
40 Livingstone, S. and Mason, J. (2015, September). Sexual rights and sexual risks among youth online. 10.
41 Internet Watch Foundation. (2020, April). The Why. The How. The Who. And the Results. The Internet Watch Foundation Annual Report 2019. 57.
42 Bracket Foundation. (2019). Artificial intelligence: Combating online sexual abuse of children. 10.
43 International Justice Mission. (2020, May). Online sexual exploitation of children in the Philippines: Analysis of recommendations for governments, industry and civil society. 7.
44 NetClean. (2019). The NetClean Report 2019: Insight two. Victims of live-streamed child sexual abuse.
45 EUROPOL. (2019, 9 October). Internet Organised Crime Threat Assessment 2019. 33.
46 Baines, V. (2019). Online child sexual exploitation: Towards an optimal international response. 30-31.
47 ECPAT International. (2018). Trends in online child sexual abuse materials. Bangkok: ECPAT International. 6.

and investigating CSAM cases as it increases offenders' anonymity. Increased anonymity is also possible with Bitcoins and other cryptocurrencies which can be used, untraceably, by OCSE offenders.[48] Conversely, artificial intelligence is defined as "the technological development that is having the single most impact on child sexual abuse investigations"[49] as tools applying this technology could, for example, analyse suspect materials on a bigger scale and higher speed compared to human analysts.[50]

While ICTs are an enabling factor, a range of socio-economic and cultural drivers are at play in amplifying children's vulnerability, including the lack of protective mechanisms available, particularly in developing countries. The 2019 WeProtect Global Threat Assessment stressed that many groups are vulnerable to OCSE, however, there is heightened risk for particular populations – like LGBTQI children and children in displaced communities, including refugees and economic migrants.

48 Nouwen, Y. (2017). Virtual currency uses for child sex offending online. ECPAT Journal Issue. 12. 4-13.
49 NetClean. (2019). NetClean Report 2019: A report about child sexual abuse crime. 36-37.
50 Bracket Foundation. (2019). Artificial intelligence: Combating online sexual abuse of children. 14.

PRIORITY ACTIONS

ECPAT International's victim-centered approach to addressing OCSE is anchored in promoting a comprehensive, multi-sector, coordinated and transnational framework which engages an array of partners and institutional actors and puts the protection of children at the very centre of collective action.[51]

Drawing on the Model National Response adopted by the We Protect Global Alliance, ECPAT's approach to eradicating OCSE rests upon a two-fold strategy addressing both the demand and supply sides. As part of this perspective, at a minimum, the following five actions are considered paramount:

1. **Specific and comprehensive legal frameworks;**
2. **Rapid and effective international cooperation and law enforcement responses;**
3. **Strategic private sector commitment;**
4. **Sustained education focusing on digital culture change amongst youth;**
5. **Specialised and long-term support and improved access to justice for child victims and survivors.**

The following sections outline the justification for each action and provide specific recommendations and examples of good practice. Besides supporting and complimenting the implementation of the WeProtect Model National Response, advancing this strategy will be of great significance in fulfilling all Sustainable Development Goals and targets directly related to the sexual exploitation of children (i.e. 5.2, 5.3, 8.7 and 16.2).

51 ECPAT International. (2015). ECPAT International submission to the Office of the High Commissioner for Human Rights. Annual discussion on rights of the child. Sexual exploitation of children and information and communication technologies.

SPECIFIC AND COMPREHENSIVE LEGAL FRAMEWORKS

We know that the development of an advanced and uniform legislation is a first essential step for states to end impunity of offenders and protect children from online sexual exploitation. Laws establishing OCSE offences in alignment with international and regional legal standards provide a common framework for successful investigation and prosecution while enabling reporting, prevention and access to justice of child victims.

An increasing number of governments have engaged in reforms to strengthen their legal frameworks against a wide range of criminal conducts encompassed under the umbrella term of OCSE. Based on model legislation on CSAM, the International Centre for Missing and Exploited Children has conducted regular global reviews of laws against CSAM related offences that shows marked progress in recent years. Indeed, while in 2006 only 27 out of 184 INTERPOL member states had sufficient legislation to combat CSAM offences, in 2018 this number had grown to 118.[52] Despite this positive development, 18 countries had no legislation at all while 62 had insufficient legal provisions to tackle CSAM.[53] These reviews do not only cover the actual criminalisation of conduct associated with CSAM (e.g. mere possession, knowingly viewing, etc.) but also provisions imposing duties on different entities, such as the mandatory reporting for Internet Service Providers, financial companies, healthcare and social services professionals etc. as well as the requirement to retain and preserve data by Internet Service Providers.[54]

As jurisdictions in which individuals can readily evade the reach of law enforcement are still many, there is a need to close loopholes in legislation to combat CSAM. Remaining gaps include the lack of a definition of CSAM encompassing computer/digitally generated child sexual abuse material,[55] the absence of specific CSAM technology-facilitated child sexual offences and the lack of legislation criminalising the mere possession of CSAM.[56]

Some efforts are underway to develop national legislation that allows punishment for an evolving range of OCSE offences. For example, in 2017, the UK enacted a progressive anti-grooming law that makes it illegal to engage in sexual messaging with a child under any circumstances.[57] However, an International Center for Missing and Exploited Children global review examining laws on online grooming of children for sexual purposes found that, as of 2017, only 63 out of 196 countries analysed had adopted some legal measures to tackle this specific criminal conduct.[58]

52 International Centre for Missing & Exploited Children. (2018). Child sexual abuse material: Model legislation & global review. Ninth Edition. 5.
53 *Ibid.*
54 *Ibid.*
55 *"Computer-generated child sexual abuse material is the production, through digital media, of child sexual abuse material and other wholly or partly artificially or digitally created sexualised images of children."* Interagency Working Group on Sexual Exploitation of Children. (2016). Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse. 40.
56 International Centre for Missing & Exploited Children. (2018). Child sexual abuse material: Model legislation & global review. Ninth Edition. 5.
57 UK Public General Acts. (2015). Serious Crime Act 2015. Section 67 as amended in 2017.
58 International Centre for Missing & Exploited Children. (2017). Online Grooming of Children for Sexual Purposes: Model Legislation & Global Review. 7.

Globally, there is considerable work still to be done to ensure that legislation in all countries adequately protects children from online grooming, regardless of whether the offender intends to meet the child offline.

Despite the alarming rise of online live streaming of child sexual abuse, existing legislation is generally inadequate to tackle this threat. This is partly due to the absence in relevant international and regional conventions of a specific and explicit provision criminalising this practice, which has emerged after these international instruments were adopted. For example, as of October 2020, none of 14 countries in Southeast Asia and Eastern and Central Africa that are part of an ongoing multi-partner research project on online sexual exploitation and abuse, Disrupting Harm, have enacted provisions to punish live streaming of child sexual abuse.[59] There is emerging jurisprudence which shows the complexities and nuances of prosecuting cases where sexual crimes are committed by offenders through a computer device without involving hands-on contact abuse with the victims. For example, in Sweden in 2017 a man was convicted of rape for remotely manipulating children into performing sexual acts via live streaming.[60]

Additional national legislation is required to criminalise the specific offence of live streaming of child sexual abuse.[61]

Some countries are adopting laws prohibiting the sexual extortion and non-consensual dissemination of sexual images, also known as "revenge porn." But with few exceptions, these laws rarely include children as victims. Instead, the preferred approach that many states are taking to address the sexual extortion of children is to apply legislation against CSAM (selling, transmitting, disseminating).[62] However this is resulting in the circumstances that young people who have made or shared self-generated sexual content consensually amongst peers are prosecuted under laws to address CSAM.

The debate around the criminalisation of young people is connected to self-generated sexual content. As in the case of 'revenge porn', in most countries sexting is currently governed by and punished under CSAM laws. In the UK, for example, a 2019 report by the University of Suffolk commissioned by the Marie Collins Foundation found that "children, some under the age of 14, are still being arrested for 'youth sexting' despite police guidance against action that leaves them with a criminal record." Child protection experts have widely criticised this approach for being too punitive.[63] Conversely, in 2018, the state government of New South Wales in Australia enacted legislation that provides a legal exception for children under 18 taking, sharing or keeping nude photographs of themselves, particularly if the sexting is consensual.[64]

Children who willingly produce sexual images representing themselves should never be held criminally liable. When this material is generated with consent or as a result of coercion, blackmailing or pressure against the will of the child, and is distributed, disseminated or sold, those responsible for the criminal conduct must be punished rather than the victims.

Comprehensive and globally harmonised legislation is crucial to improve the effectiveness of multijurisdictional investigations against OCSE. Its absence does contribute to the emergence of "safe havens" for offenders, who concentrate their activities in countries with more lenient legislation. Also, since the cross-border nature of OCSE requires international law enforcement cooperation, the lack

59 Final national and regional reports to be published in late 2021.
60 Swedish Prosecution Authority. (2018). Hovrättsdom i uppmärksammat sexualbrottsärende. [Translated from Swedish].
61 Dushi, D. (2019). Combating the live streaming of child sexual abuse and sexual exploitation: A need for new legislation.
62 Neris, N., Pacetta Ruiz, J. & Giorgetti Valente, M. (2018). Fighting the dissemination of non-consensual intimate images: A comparative analysis.
63 Murray, L. et al. (2013). 'Let's get sexting': Risk, power, sex and criminalisation in the moral domain. *International Journal for Crime and Justice.* Brisbane Vol. 2, Fasc. 1, (2013): 35-49.
64 New South Wales Government. (2018). New legislation to strengthen child sexual abuse laws. Factsheet for service providers. 3.

of harmonised legislation hampers these efforts due to different categorisation of criminal conducts across jurisdictions. Child rights organisations play a critical role in identifying loopholes in the legal framework and urging governments to make appropriate legal reforms, an example being the Declaration for the Protection of Children from All Forms of Online Abuse and Exploitation in ASEAN Member States, adopted by all Heads of States during the 35th ASEAN Summit in November 2019, developed with the technical support of ECPAT International and UNICEF East Asia and Pacific Regional Office.

Given the constant developments of ICTs, legal provisions must be flexible and as technology neutral as possible to encompass any type of digital means used to commit OCSE offences. Furthermore, laws must be rapidly reviewed and adapted to keep pace with evolving criminal conducts.[65] Other areas of concern which would require law amendments beyond substantive legislation criminalising OCSE related conduct are procedural approaches and regulations needed to protect child victims and ensure the likelihood of successful investigations. These include: laws and procedures on data retention and preservation, legal duties and responsibilities for Internet Service Providers and regulations on undercover investigations.

It is imperative to advocate for domestic legislation fully in line with international and regional standards[66] and for the adoption of consistent definitions and terminology following the 'Luxembourg Guidelines'.

65 Committee on the Rights of the Child. (2019, 10 September). Guidelines. Para. 19. See also: ECPAT International. (2019). Explanatory report to the Guidelines regarding the implementation of the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography. 29.

66 The most relevant regional and international treaties to fight OCSE are: the *OPSC on the Sale of Children, Child Prostitution and Child Pornography, the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse* and the *Council of Europe Convention on Cybercrime.*

RAPID AND EFFECTIVE INTERNATIONAL COOPERATION AND LAW ENFORCEMENT RESPONSE

We know that streamlined cooperation and information exchange among law enforcement agencies across countries are pivotal to ensure a speedy victim identification and rescue process as well as an effective prosecution of offenders. Successful investigations of OCSE offences also demand specialist law enforcement capacity, tools and training, and need to be supported by adequate human and financial resources.

Robust legal frameworks, while extremely important, are not sufficient by themselves to address OCSE. Effective policing of these crimes requires, in the first place, specific expertise in ICTs and digital forensics. Indeed, the misuse by some offenders of encryption technologies, anonymity tools, or alternative payment methods may complicate traditional police methods of investigation and entail the use of highly technical tools and specialised knowledge.

Law enforcement agencies need to be equipped with the necessary technology and resourced with trained staff to investigate OCSE crimes, identify victims, remove CSAM/CSEM and detect any other suspicious behaviors potentially harmful to a child.

However, institutional capacity and resources vary considerably across countries and even within countries, and most national agencies work with limited resources facing growing volumes of CSEM available online. This frequently means that law enforcement is forced to prioritise investigations, with only a fraction of reported cases able to be investigated. From the 60 countries in the Out of the Shadows Index, just 34 have a designated law enforcement agency or unit to counter SEC, some of which are dedicated to combating OCSE, but only eight have allocated a dedicated budget to online cases.[67]

Law enforcement specialisation against OCSE is of great importance but should not be pursued in isolation. A more holistic approach that incorporates knowledge and techniques into the investigation of all 'online' and 'offline' crimes against children is needed to better address increasingly interlinked contact and non-contact offences.[68]

OCSE crimes are typically borderless, and perpetrators may even be in different countries

67 The Economist Intelligence Unit. (2019). Out of the Shadows: Shining light on the response to child sexual abuse and exploitation.

68 ECPAT International and INTERPOL. (2018). Towards a global indicator on unidentified victims of child sexual exploitation – Summary Report. 15.

to their victims. This also means perpetrators can use borders to their advantage, to move their operations to evade investigation, or to find legal contexts that suit their criminal intent. Law enforcement is typically national – designed to uphold states' own legal frameworks, and not well structured to facilitate international information sharing and cooperation, so multiple barriers must be overcome in order for services to collaborate. For borderless crime, a borderless response is necessary. International investigative coordination contributes to more efficient operational activities whereby police units can join forces, increasing opportunities to identify and rescue more victims and arrest more offenders across multiple jurisdictions. It also reduces the duplication of efforts – like different national forces searching for victims or perpetrators that have already been arrested elsewhere.[69] Regrettably, cooperation across jurisdictions can face several practical challenges due to different legal frameworks, operational procedures, inconsistent definitions of OCSE offences in different jurisdictions, discrepancies in available resources and capacity across law enforcement agencies, as well as language and cultural barriers.[70]

International collaboration therefore plays a vital role in improving the effectiveness of national law enforcement agencies to tackle the global OCSE problem. The Virtual Global Taskforce, is an example of an international alliance comprised of law enforcement, industry and non-government partners dedicated to the protection of children from online sexual exploitation and abuse. EUROPOL, the European Union's law enforcement agency, includes sexual exploitation of children as one of the main crime areas it focuses upon. Beyond investigating work conducted with national law enforcement agencies, EUROPOL implements specific campaigns and activities aimed at curbing OCSE, such as the Stop Child Abuse - Trace an Object campaign, which gives the public the opportunity to view objects portrayed in CSAM and provide clues about their origin and possible location. INTERPOL is the only global law enforcement agency. INTERPOL's mandate includes to support the fight against OCSE and as such it has developed several initiatives in this field. An example is the IWOL lists (INTERPOL worst-of list) which lists known domains (i.e. the address/name of a website) containing very severe CSAM/CSEM to be shared with Internet Service Providers willing to reduce the availability of this kind of material in their platforms.

Steps must be taken to facilitate cross-jurisdictional investigations. There is a need to harmonise approaches to the sharing of case-related information on child victims of online sexual abuse and exploitation within and between countries,[71] including through cooperation agreements enabling secure use and sharing of data.[72] Efforts at international level should also be made to implement a single standard framework for a uniform classification of CSAM.[73]

69 Baines, V. (2019). Online child sexual exploitation: Towards an optimal international response. 23.
70 Macilotti, G. (2020). Online child pornography: Conceptual issue and law enforcement challenges. In Balloni, A., Sette, R. (eds.). Handbook of research on trends and issues is crime prevention, rehabilitation and victim support. 231.
71 ECPAT International and INTERPOL. (2018). Towards a global indicator on unidentified victims of child sexual exploitation – Summary Report. 15.
72 Bracket Foundation. (2019). Artificial intelligence: Combating online sexual abuse of children. 5.
73 Child Dignity Alliance. (2018). Technology Working Group Report. 6.

INTERNATIONAL CHILD SEXUAL EXPLOITATION DATABASE

The International Child Sexual Exploitation database (ICSE) is hosted by INTERPOL and contains over 2.7 million child sexual abuse items uploaded by and on behalf of INTERPOL member countries. The ICSE database is an intelligence and investigative tool, which allows investigators to share information and data with colleagues across the world to help identify and locate child victims of online sexual exploitation and potential offenders. The ICSE database enables analysis and comparison of CSAM/CSEM, using image and video comparison software which allow law enforcement to make connections between cases and avoid duplications. Users of the ICSE database, who need to be either trained and certified law enforcement agents or accredited non-law enforcement analysts - can organise their submission to the ICSE database by grouping them by series of images and/or videos or by investigations.[74] Labelling identified images and videos (assigning hashes, see box below) improves efficiency by preventing already identified images from having to again be viewed and analysed, and prevents solved/closed cases from being unnecessarily re-investigated. National repositories of CSAM held by national law enforcement agencies can also be connected to the ICSE database.[75]

All governments should consider establishing a national database of CSAM and connect it internationally to the INTERPOL ICSE database. The number of countries accessing and linked to this database must be expanded to facilitate case initiation and cross-border investigation.[76]

Resources for victim identification programmes must also be secured and prioritised in relevant national action plans and regional policy frameworks and efforts.[77]

Multi-stakeholder initiatives are also key in assisting states which are currently less proficient in OCSE law enforcement by providing specialised training, sharing best practices and sophisticated investigative tools.[78] A valuable example of partnerships of this kind is the Philippines Internet Crimes Against Children Center, established in February 2019 through cooperation among the Philippines national police, the Australian Federal Police, the UK's National Crime Agency and the International Justice Mission. In its first year of activity, the Philippines Internet Crimes Against Children Center managed 41 operations leading to the rescue of 136 victims and children at risk of sexual exploitation online and the arrest of 41 offenders. Similarly, in March 2019, the Anti-Human Trafficking and Child Protection Unit of the Directorate of Criminal Investigations of the Republic of Kenya, was launched with the support of the United Nations Office on Drugs and Crime and the UK's National Crime Agency.[79,80] The unit includes a forensic lab to triage seized devices and it is connected to the ICSE database.[81]

74 ECPAT International and INTERPOL. (2018). Towards a global indicator on unidentified victims of child sexual exploitation – Technical Report. 6.
75 *Ibid.*, 5.
76 *Ibid.*, 15.
77 *Ibid.*, 16.
78 Human Rights Council. (2014). Report of the Special Rapporteur on the sale of children, child prostitution and child pornography. ICTs and SEC Thematic Report. 18.
79 UNODC. (2019, 25 March). Official Launch of the Anti-Human Trafficking and Child Protection Unit based at the Directorate of Criminal Investigations Academy.
80 UK Government. (2020, 1 March). UK backed Anti-Human Trafficking Child Protection Unit opened at the Kenyan coast.
81 UNODC. (2019, 25 March). Official launch of the Anti-Human Trafficking and Child Protection Unit based at the Directorate of Criminal Investigations Academy.

STRATEGIC PRIVATE SECTOR COMMITMENT

We know that the private sector has both the responsibility and capabilities to help address OCSE. In collaboration with governments, law enforcement and civil society, the ICTs sector, tech industry and financial sector are able to develop innovative solutions that can thwart attempts by online child sex offenders to circumvent detection and investigation as well as better detect and take down CSAM/CSEM content. Technological solutions can also ensure more effective and efficient responses to evolving forms of OCSE.

The misuse of various legitimate technologies has enabled perpetrators to access and contact victims, distribute and share CSAM and even communicate and collaborate with each other on ways to avoid detection and hone their techniques.

A key concern impacting children's safety currently is the widespread adoption of end-to-end encryption by many tech platforms. Intended by tech companies as a mechanism to address legitimate privacy concerns when using their platforms, major tech companies such as Facebook, Google and Apple have identified this method as the best solution to address these concerns.[82] However, the technology has the maleficent impact of protecting the anonymity and privacy of perpetrators committing OCSE crimes as well. Many technology platforms such as Line, Skype and WhatsApp have provided encrypted services for some time and Facebook recently announced the implementation of end-to-end encryption on its Messenger.[83] Many child protection agencies have vocally criticised Facebook's encryption plans, highlighting that this move would pose serious challenges for investigations and prosecutions, enabling perpetrators to act anonymously and stopping the ability of Facebook to proactively detect millions of instances of CSAM content on its Messenger platform as it currently does – in 2018, the National Center for Missing and Exploited Children received a total of 18.4 million reports. Of this, 90% were from Facebook (16.8 million) and of those, 12 million (71.4%) came from Facebook Messenger.[84] It is argued that this content would 'go dark' with encryption. It will also considerably limit the ability of law enforcement to detect suspicious behaviors towards children and collect evidence that is known to happen on Facebook Messenger.[85]

Among its adverse effects and in addition to the one mentioned above, encryption is known to hamper the efficacy of technologies such as PhotoDNA, which have been instrumental in recent progress to efficiently detect and remove online CSAM. Considering that over 50% of Internet traffic is already encrypted,[86] companies have an obligation to invest in the development and deployment of systems and tools that can aid investigations and detection of CSAM and other harmful behaviors in their end-to-end encrypted platforms that are as efficient as systems relying on content detection operating in non-encrypted environments. In 2020, the European Commission has announced the creation of a technical expert process within the European Union Internet Forum to find possible ways for companies to detect and report child sexual abuse in end-to-end encrypted electronic communications, which respects fundamental rights

82 Kleinman, Z. (2019, 30 April). Facebook boss reveals changes in response to criticism. *BBC News;* Yun Chee, F. (4 June 2019). Google faces privacy complaints in European countries. *Reuters;* (26 November 2019). Reed, A. (26 November 2019). Apple update for user privacy fuels questions and criticism. *Seattle Times.*

83 Mark Zuckerberg. (2019, Mar 7). A privacy focused vision for social networking.

84 Dance, G & Keller, M. (2019). The Internet is overrun with images of child sexual abuse. What went wrong? *The New York Times.*

85 ECPAT International, NSPCC, National Center for Missing and Exploited Children et al. (6 February 2020). ECPAT network urges Facebook to re-think encrypting Facebook Messenger.

86 Bracket Foundation. (2019). Artificial intelligence: Combating online sexual abuse of children. 7.

and is cautious to not create new vulnerabilities criminals could exploit.[87]

While users of online services have a legitimate interest in ensuring that their data is protected, children's and victims' privacy must remain the priority.

Numerous strategies to prevent and address OCSE crimes through technology platforms have been identified. These include 'splash pages' and deterrence messages that pop-up when certain topics are searched, pre-screening of material (by comparing with PhotoDNA) before upload and download of any images, artificial intelligence chat moderation and promotion of reporting mechanisms and requirements to identify, block and remove CSAM immediately when detected.[88,89]

In 2020, the Technology Coalition, a group of 18 global tech companies,[90] launched a new multi-layer plan to eradicate OCSE which will lead, among other things, to the creation of a multi-million dollar investment in an Innovation Fund.[91]

PHOTODNA

PhotoDNA is a hashing technology developed in 2009 by Microsoft in collaboration with Dartmouth College. It is an automated system that assigns a 'hash' (i.e. a unique digital fingerprint) to an image that has been identified as CSAM. This then means further copies of this image can be identified without the need to view and analyse the image. Companies and organisations all around the world can quickly compare and match millions of photos against a hash of known illegal content.[92] This helps identify copies of known child sexual abuse images wherever they have been distributed online, and even if they have been modified. Now also applicable to videos, PhotoDNA is a fully automated and completely free tool. Law enforcement agencies also use PhotoDNA for the purpose of investigation.[93] Further, based on image and video hashing, Project Vic, a coalition of law enforcement and private sector partners, has developed innovative tools that have helped identity and rescue thousands of child victims worldwide.

Building on existing good practices, the technology industry including content and social media providers should increase industry cross-collaboration to co-create and deploy advanced technical solutions.

The deployment of innovative solutions in partnership with NGOs and law enforcement, paying particular attention to evolving forms and trends in OCSE, is the best model forward.

87 European Commission. (2020, 24 July). Communication from the commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. EU Strategy for a more effective fight against child sexual abuse.
88 IWG_OSO. (2019). Best practice in the management of online sex offending. 19.
89 ECPAT International. (2016). Power, impunity and anonymity. 75-76. See also: IWG_OSO (2019). Best practice in the management of online sex offending. 19.
90 Companies that are part of this initiative include among others, Facebook, Amazon, Apple, Microsoft, Google, PayPal, Snapchat, Adobe and GoDaddy.
91 GSMA. (2020, 10 June). Technology Coalition announces project to protect children from online sexual exploitation.
92 ECPAT International. (2016). ECPAT Internet and Technology Factsheet. What are Hashes? What is PhotoDNA?
93 Thorn staff. (2016, 25 April). Microsoft's PhotoDNA: Leading the fight against child sexual abuse imagery.

Some of the safety features can be tailored to country level specificities for especially vulnerable groups such as girl adolescents and women.[94]

Some of the safety features that can be put in place can include in-built blocking solutions for illegal content at device level.[95]

Although there are some good examples from companies and some self-regulatory measures, industry engagement to keep children safe online remains generally insufficient. Many more efforts are required from a wide range of interactive platforms (such as gaming and social interaction platforms largely used by children) to ensure they take action against OCSE by vigorously detecting and eliminating CSAM as well as suspicious behaviours targeting children.[96] In particular, a greater involvement is necessary from the gaming sector, which, based on our work experience, appears to have been limited so far.

With regards to the financial sector, outstanding industry initiatives that are contributing to deliver a suitable response to OCSE include the Financial Coalitions against Child Sexual Exploitation and its regional and national chapters in Asia-Pacific and the US, which brings together leading companies from the financial sector to eliminate OCSE by impeding payments for illegal material.

The involvement of online payment services, money transfer services and cryptocurrency providers is especially key to undermine the business model of offenders and criminal networks in cases of commercial forms of OCSE such as live streaming of child sexual abuse and sexual extortion.

Governments must legislate specific actions from companies to hold them accountable when their platforms or services are misused in ways that can be foreseen to cause lasting damage to children. This strategy has already been adopted in many countries. This encompasses a broad range of areas such as mandatory reporting of illegal content and procedural laws around digital evidence and data retention. According to an International Center for Missing and Exploited Children global review released in 2018, 32 states have established a legal obligation for Internet Service Providers to report suspected CSAM to law enforcement or some other mandated agency.[97] The UK 2019 Online Harms White Paper provides a strong example of a regulatory framework that could guide such legislative action.

Governments must introduce legislative measures to ensure that Internet Service Providers, tech companies and other online service providers have a (legal) responsibility for reporting, controlling, blocking and removing CSAM and detecting and reporting harmful behaviours to children.[98]

The opportunity to enact legislation requiring hardware manufacturers and providers of online services and social media platforms to implement more stringent age verification techniques on all relevant devices should also be explored.[99]

94 Bracket Foundation. (2019). Artificial intelligence: Combating online sexual abuse of children. 17.
95 For more information see: Safety by Design Initiative, Australian eSafety Commissioner: https://www.esafety.gov.au/about-us/safety-by-design
96 Bracket Foundation. (2019). Artificial intelligence: Combating online sexual abuse of children. 30.
97 International Centre for Missing & Exploited Children. (2018). Child sexual abuse material: Model legislation & global review. Ninth Edition. 36-59.
98 Committee on the Rights of the Child. (2019, 10 September). Guidelines. Para. 41.
99 Independent Inquiry Child Sexual Abuse. (2020). The Internet investigation report March 2020. 102.

SUSTAINED EDUCATION FOCUSING ON THE DIGITAL CULTURE CHANGE AMONGST YOUTH AND ASSOCIATED ONLINE RISKS

We know that empowering children, young people, parents, carers and teachers with the skills and knowledge for responsible and safe use of ICTs reduces the likelihood of getting entrapped in risky situations and helps children make more informed decisions when engaging in online interactions. Educational efforts are more impactful when they don't only focus on risks, but encourage open communication and are tailored to reflect children's evolving capacities.

The digital age has brought with it several cultural transformations. With Internet use by children becoming more personal, more private and less supervised,[100] the easy access to unlimited pornography online, much of which may feature readily available violent/hard-core content, may have led to the desensitisation of young people towards pornographic material and emerging risky online sexual behaviors.[101]

The evidence indicates that children are increasingly posting self-generated material of themselves online that is sexual in tone,[102] which has been confirmed by law enforcement sources who have witnessed an increase of self-produced materials in seized CSAM collections.[103] While research suggests that girls feel pressured or coerced into sexting more often than boys,[104] this phenomena will continue to impact all genders.[105] The notion of "coercion" is difficult to capture and understand especially for law enforcement specialized in victim identification. Multiple contexts when this type of content can be produced are challenging the traditional binary categorisation between CSAM and what is considered "self-produced" material.

However, pictures taken and shared consensually between peers that are never shared further do not necessarily have negative consequences. A small study on self-generated sexual images conducted by ECPAT Sweden, in which 37 children were asked about their views on the topic, found that many children consider that self-produced images provide advantages in their relationships and/or increased self-esteem.[106] However, when the materials are forwarded without consent or acquired and distributed by offenders, the impact on the child may have a range of negative impacts.[107] Furthermore, the normalisation of sexual content, both in terms of images and sexualised online conversations, may lead to victims underreporting because they may fail to perceive what is happening to them as abusive or exploitative.[108]

Finally, education approaches need to acknowledge that these digital risk scenarios are here to stay and we need to help children prepare to negotiate

100 UNICEF. (2017). The State of the World's Children 2017: Children in a Digital World. 1.
101 Palmer, T. (2015). Digital Dangers: the impact of technology on the sexual abuse and exploitation of children. *Barnado's. 35.*
102 Madigan S., et al. (2018). Prevalence of multiple forms of sexting behavior among youth: A systematic review and meta-analysis.
103 Internet Watch Foundation. (2020, April). The Why. The How. The Who. And the Results. The Internet Watch Foundation Annual Report 2019. 57.
104 K. Cooper et al. (2015). Adolescents and self-taken sexual images: A review of the literature. 22.
105 Livingstone, S. and Mason, J. (2015, September). Sexual rights and sexual risks among youth online. 10.
106 ECPAT Sweden. (2020, May). "I början vart det lite läskigt men nu är det vardag" En rapport om yngre barn och egenproducerat material. [Translated from Swedish].
107 International Centre for Missing and Exploited Children. (2018). Studies in child protection: Sexual extortion and nonconsensual pornography. 36.
108 Palmer, T. (2015). Digital Dangers: the impact of technology on the sexual abuse and exploitation of children. *Barnado's.* 35.

and mitigate them. A 2014 review of ten online educational campaigns to address sexting found that these interventions "typically rely on scare scenarios, emphasise the risk of bullying and criminal prosecution, engage in female victim blaming and recommend complete abstinence from sexting."[109] The overall negative understanding of sexting and the stigmatisation of children engaging in this practice, including in media reports, must be prevented, so that they do not feel ashamed to speak out if they find themselves in a risky situation online.[110] There is a need to recognise that sexting can be part of normal sexual development. When developing sexting risk prevention programmes within and beyond educational settings, it is therefore imperative to adopt a gender-sensitive, evidence-based and rights-centred approach that acknowledges both adolescents' vulnerability and sexual agency.[111]

Education focusing on aspects of our fast-changing digital culture and the risks this may facilitate for young people is critical, yet it remains limited, not fit-for-purpose and/or under-resourced. A lack of political will to address the prickly topic of sexuality for children and young people results in a persisting reluctance by parents and society at large to speak to young people about sexuality in honest and risk minimising ways.[112]

There is a need to integrate comprehensive and age appropriate sexual education that addresses cultural aspects of the digital world like consent, notions of privacy, pornography use and sexting into sexual health and development curriculums for children and adolescents.

Discussions should extend to relationship issues, such as consent, power dynamics and potential abuse by peers and intimate partners. Open dialogue about these practices between students and teachers as well as between children and parents must be actively fostered.[113]

There is a need to develop non-formal education programmes to reach "unconnected children" that are at high risk of sexual exploitation with the subsequent digitalisation of the evidence, including those living in remote rural communities or on the street and those from under privileged or marginalised communities.[114]

109 Döring, N. (2014). Consensual sexting among adolescents: Risk prevention through abstinence education or safer sexting. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace,* 8(1). 1.
110 Setty, E. (2019). A rights based approach to youth sexting: Challenging risk, shame, and the denial of rights to bodily and sexual expression within youth digital sexual culture. *International Journal of Bullying Prevention* 1: 298–311.
111 Döring, N. (2014). Consensual sexting among adolescents: Risk prevention through abstinence education or safer sexting. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace,* 8(1). 1.
112 IWG_OSO. (2019). Best practice in the management of online sex offending. 19.
113 Jørgensen, C. et al. (2018). Young people's views on sexting education and support needs: findings and recommendations from a UK-based study. *Sex Education.* 19: 1-16.
114 *Ibid.*

SPECIALISED AND LONG-TERM SUPPORT AND IMPROVED ACCESS TO JUSTICE FOR CHILD VICTIMS AND SURVIVORS

We know that children whose sexual exploitation has an online component face unique barriers in accessing justice. Helping child victims and survivors to engage with the justice system more effectively is pivotal for their recovery. It is essential that the provision of specialised and sustained support is coupled with this approach to ensure that their right to access justice and remedies are fulfilled, but will also contribute to addressing the trauma they experience and facilitate a return to a sense of normalcy quickly.

A growing body of literature shows that OCSE has several specific psychological effects on victims beyond the ones we would expect from a victim of forms of non-tech related sexual violence. The fear that sexual images could be shared online and may be viewed well into the future intensifies feelings of shame, humiliation and vulnerability. Many young people also blame themselves for the abuse, especially when they may have created images themselves, or if school, peers and family adopt unsupportive approaches once their abuse has been disclosed.[115] ECPAT research on accessing justice found that the fear that recordings of their abuse may be discovered is so intense among children used in online CSAM or live performances that it makes them even more reluctant to report than other SEC victims.[116]

Helplines and hotlines are effective mechanisms to facilitate reporting of OCSE crimes. They enable access to support services confidentially and safely while also contributing to reducing the amount and circulation of CSAM through pursuing takedowns. They are also an important outreach and awareness mechanism for children and communities, providing information and services. Consistent efforts have been made in recent years to develop and rollout hotlines and helplines in many countries (such as via the INHOPE network or the Internet Watch Foundation). Child Helpline International brings together 178 child helplines from 146 countries in its network. A report released by Child Helpline International and UNICEF in 2016 exposed a number of challenges that existing helplines are facing, including a lack of advanced training for operators and the absence of protocols for how to handle and refer cases of online abuse and exploitation.[117]

Every country must have robust and sustainable hotline and helpline services for children with staff specially trained to respond to OCSE. Campaigns to advertise the existence of this mechanism are also needed to increase access to such services.[118]

Like most forms of sexual violence, OCSE crimes are assumed to be chronically under-reported with most children experiencing it unlikely to be

115 Hamilton-Giachritsis, C. et al. (2017). "Everyone deserves to be happy and safe": A mixed methods study exploring how online and offline child sexual abuse impact young people and how professionals respond to it. 30-31.
116 ECPAT International. (2017). Through the eyes of the child: Barriers to access to justice and remedies for child victims of sexual exploitation. 21.
117 Child Helpline International. (2016). A new reality: Child Helplines report on online child sexual exploitation and abuse from around the world. 17.
118 *Ibid*., 26.

identified or connected with the justice system. Even when they do engage with it, existing child friendly procedures may not be well suited to their needs. For example, ECPAT research indicates that there are currently few explicit restrictions on the disclosure and discovery by the parties of sexual abuse imagery in evidence.[119] Additionally, given the very abuse they have experienced likely involved filming, many child victims may feel uncomfortable being filmed in court as they describe their traumatic experiences. While technology provides a positive opportunity for children to give testimony remotely from their perpetrators or the courtroom, this may not always be the best option.[120]

Governments may consider adopting specific measures to reduce secondary trauma for children in these cases. These may include: evidentiary protections that restrict disclosure and admission into evidence of CSAM; specific protocols for interviews and examination of child victims; and specialised interview and trial procedures that consider each child's views and best interests before making use of camera equipment or digital technologies. [121]

To improve access to justice for children who have experienced online sexual exploitation, provisions tailored to respond to their special needs should be established. Judges, lawyers and prosecutors working on child-related cases should be appropriately trained to deal with OCSE cases and child victims of this crime.

Child victims of online exploitation also face peculiar challenges in realising their right to compensation. Given the nature of these crimes, child victims might not even know the identity of the perpetrator or may not be aware that they are victims.

Moreover, the losses they suffer may not be easily quantifiable as images may be circulated online indefinitely and viewed by countless offenders.[122] Not surprisingly, compensation is not generally paid by either perpetrators or states.[123]

Once identified, children must be notified not only of their right to seek compensation, but especially and fundamentally that they are a victim.[124] Countries need to establish state managed compensation schemes so that all child victims of online sexual exploitation can be compensated regardless of whether the perpetrator has the means to pay.[125]

THE AMY, VICKY, AND ANDY CHILD PORNOGRAPHY VICTIM ASSISTANCE ACT

Under a US federal law passed in 2018 called the Amy, Vicky, and Andy Child Pornography Victim Assistance Act, every child victim of online sexual exploitation is entitled to receive at least US$3,000 from every offender possessing a sexual image depicting him/her. Because the rate of restitution has been standardised, it is now easier for courts to establish an amount for compensatory damages. The new law also gives child victims access to the images that the convicted criminals possessed.[126]

119 ECPAT International. (2017). Through the eyes of the child: Barriers to access to justice and remedies for child victims of sexual exploitation. 21.
120 *Ibid.*
121 *Ibid.,* 159-160.
122 ECPAT International. (2017). Barriers to compensation for child victims of sexual exploitation: A discussion paper based on a comparative legal study of selected countries. 33.
123 UNICEF. (2016). Victims Are Not Virtual: Situation assessment of online child sexual exploitation in South Asia. 44.
124 ECPAT International. (2017). Barriers to compensation for child victims of sexual exploitation: A discussion paper based on a comparative legal study of selected countries. 24.
125 *Ibid.,* 50.
126 ECPAT International. (2018, 14 December). US: New law will ensure full compensation for victims of online child sexual exploitation.

The fact that a permanent record exists of the child's abuse in OCSE cases impacts the recovery and reintegration process and may increase the need for long-term psychological counselling and social services. There is evidence that some progress has been made in service provision for child victims of online exploitation. A 2017 review by the International Center for Missing and Exploited Children found that 111 out of 161 countries analysed provided some support services to children for OCSE.[127] However, the level of specialisation of such assistance remains unknown or limited. For example, ECPAT research in Thailand, Philippines and Nepal in 2017 identified a lack of specialised, comprehensive and integrated care (both short-term and long-term) for children who experienced OCSE.[128]

Specialised, long-term support services for child victims of Internet based sexual exploitation must be integrated into existing programmes. Since OCSE presents particular impacts and potential traumas, therapies need to be adapted to their needs and include other approaches apart from trauma focused behaviour therapy.[129]

127 International Centre for Missing and Exploited Children. (2017). Framing implementation. A supplement to child pornography: model legislation and global review. 4.
128 ECPAT International. (2017). Casting light on the care, recovery and (re)integration needs of commercially sexually exploited children from the voices of children, adult survivors and their service providers in Nepal, the Philippines and Thailand. 46.
129 ECPAT International. (2009). Child abuse images and sexual exploitation of children online. 76.

CONCLUSION

The recent sharp increases in reported cases of OCSE suggest two crucial factors. Work to increase access to the range of reporting mechanisms must continue, and globally, the extent of OCSE continues to grow. As the boundaries between the physical and digital worlds continue to blur, particularly for children growing up in the digital age, OCSE will continue to evolve and new forms emerge. Encouragingly, work is underway at national and international levels to prevent and respond to this global threat, but innovative and substantial actions are needed to keep up with this evolving problem. Legal frameworks must improve and approximate global consistency and regulation must make tech companies and Internet Service Providers accountable for action. Law enforcement must collaborate across jurisdictions, adopt sophisticated techniques and be properly equipped and funded.

There is an urgent need to further boost and sustain collective action against OCSE at this moment in time. ECPAT International has identified in this paper five areas where progress can and must be made. Again, as this problem is not confined by borders, strategic partnerships with the involvement of an increasing number of global actors will be instrumental in making this happen. As a society, we have a duty and a responsibility to stop the demand underpinning OCSE and ensure the rights of children online and offline are fulfilled.

Suggested citation:
ECPAT International. (2020). Summary Paper on Online Child Sexual Exploitation. Bangkok: ECPAT International.

328/1 Phaya Thai Road, Ratchathewi
Bangkok, 10400 THAILAND
Tel: +662 215 3388
Email: info@ecpat.org
Website: www.ecpat.org