ECPAT INTERNATIONAL
Ending the sexual exploitation of children

ECPAT International's submission to the Australian Parliamentary Joint Committee on Law Enforcement

Inquiry into law enforcement capabilities in relation to child exploitation

19 August 2021

INTRODUCTION

ECPAT International is a global network of civil society organisations, working to eradicate all forms of sexual exploitation of children. Over the past 30+ years, ECPAT has become the forefront international NGO network dedicated to end this severe form of violence against children, advocating for State accountability and more robust measures across sectors to enhance the protection of victims. ECPAT currently has 122 member organisations operating in 104 countries around the world.

This submission by ECPAT International is in response to the inquiry issued by the Australian Parliamentary Joint Committee on Law Enforcement on law enforcement capabilities in relation to child exploitation.

Trends and changes in relation to the crime of online child sexual exploitation

(Response to point a and f of the inquiry)

The shifting boundaries between the physical and digital world are changing the way we define and address 'online child sexual exploitation' - a phrase that is itself becoming obsolete as it still implies a deliberate discrete act of 'using the Internet' when in fact for most of us we are connected digitally throughout our waking hours.[1] Differentiating between 'online' and 'offline' instances perhaps does not always help us to understand, prevent or respond. Children can be exploited while they spend time in digital environments, but equally, offenders can use digital technology to access children, arrange abuse, or to share images of in-person ('offline') exploitation.[2] Preliminary data from the *Disrupting Harm* project indicates that only a small proportion of children are subjected to exclusively online child sexual exploitation and abuse. More time online does increase potential risks of children encountering offenders, and the growth in social media use, gaming and child focused online spaces creates opportunities for offenders to access and groom children.[3,4] However, exposure to risk does not automatically mean more harm with the right protections and engagement with the online world.

ECPAT noted some trends in online child sexual exploitation in our 2018 global qualitative interviews with law enforcement officers who indicated that they were seeing increasing levels of violence in the child sexual abuse material they encountered in their work and that more egregious images involved younger children and were often produced within a family context.[5] ECPAT's collaboration with INTERPOL to analyse a sample of images in the International Child Sexual Exploitation database found similar trends.[6]

[1] Livingstone, S and Stoilova, A. (2020, 5 July). Understanding children online: Theories, concepts, debates.
[2] ECPAT International. (2020). Summary paper on online child sexual exploitation. 6.
[3] NetClean. (2019). NetClean Report 2019: A report about child sexual abuse crime. 4.
[4] INTERPOL. (2020, September). Threats and trends. Child sexual exploitation and abuse. COVID-19 Impact.
[5] ECPAT International. (2018). Trends in online sexual abuse material, 5.
[6] ECPAT International and INTERPOL. (2018). Towards a global indicator on unidentified victims of child sexual exploitation – Summary Report. 4.

In terms of ethnicity, known child sexual abuse material tend to suggest that the majority of both victims and offenders are white Caucasians, however, this analysis depends on the available data sources which are highly skewed towards the developed world.[7] Forthcoming research for the *Disrupting Harm* project will help address this gap by presenting comprehensive data for 13 developing countries in Southeast Asia and Africa (national reports will be released from September 2021 to March 2022). Preliminary results from nationally representative surveys in the project show that children in developing countries report experiencing a range of potential and actual online child sexual exploitation. The data also indicates that, contrary to common concerns about strangers, the offenders are most often known to the children already.

Although girls continue to outnumber boys in known child sexual abuse materials, boys are increasingly seen to be a significant proportion of the victims. For example, INHOPE noted an increase in the proportion of boys depicted in reported child sexual abuse material from 4.3% in 2017 to 16.8% in 2018.[8] In addition, in our analysis of the material contained in the International Child Sexual Exploitation database analysis, 30.5% of images included boys, and when boys were depicted, the abuse was more likely to be severe or involve paraphilic themes and violence.[9]

Another emerging trend involves the use of entertainment tools based on virtual reality technology to contact children for the purpose of sexual exploitation.[10] 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 or captured well in legislative frameworks.[11]

Recent research funded by the Australian eSafety Commissioner on the impact of COVID-19 on online child sexual exploitation indicates that Australian law enforcement agencies, child helplines and online reporting mechanisms showed increased reporting of a range of online related child sexual abuse and exploitation.[12] This noted increase in reporting was also seen globally.[13] However, global law enforcement bodies have also noted that there is not yet evidence indicating an increase in new child sexual abuse material.[14] It could be that during movement restrictions, global attention turned to our online lives and has resulted positively in more vigilance, and more concerns being raised.

In October 2020, EUROPOL highlighted that live-streaming of child sexual abuse increased during the pandemic,[15] a possible by-product of travel restrictions curtailing travelling sex offenders.

Despite increased attention on online child sexual exploitation during this period, the COVID-19 pandemic has globally resulted in fewer reports reaching police, difficulties in moving forward with

[7] ECPAT International and INTERPOL. (2018). Towards a global indicator on unidentified victims of child sexual exploitation – Summary Report. 4.
[8] INHOPE. (2020). Annual report 2018. 24.
[9] ECPAT and INTERPOL. (2018). Towards a global indicator on unidentified victims in child sexual exploitation material. 3.
[10] Baines, V. (2019). Online child sexual exploitation: Towards an optimal international response. 30-31.
[11] *Ibid.*
[12] Salter, M, Wong W.K.T. (2021, May). The impact of COVID-19 on the risk of online child sexual exploitation and the implications for child protection and policing.
[13] See e.g. EUROPOL. (2020, June). Exploiting isolation: Offenders and victims of online child sexual abuse during the COVID-19 pandemic. National Center for Missing and Exploited Children. (2020, July). COVID-19 and missing & exploited children.
[14] INTERPOL. (2020, September). Threats and trends. Child sexual exploitation and abuse. COVID-19 Impact. 15.
[15] See e.g. EUROPOL. (2020, June). Exploiting Isolation: Offenders and victims of online child sexual abuse during the COVID-19 pandemic. National Center for Missing and Exploited Children. (2020, July). COVID-19 and missing & exploited children.

existing investigations and reduced use of the global International Child Sexual Exploitation database due to movement restrictions and other priorities faced by law enforcement personnel.[16]

Conceptual and legal considerations on online child sexual exploitation

(Response to point a and f of the inquiry)

Globally, ECPAT observes that States do not tend to do as well with defining and criminalising online child sexual exploitation offences beyond those related to child sexual abuse material.

Grooming children for sexual purposes

The Council of Europe Convention on Protection of Children against Sexual Exploitation and Sexual Abuse, also known as Lanzarote Convention provides the leading legal guidance on addressing sexual exploitation and abuse. However, the Lanzarote Committee itself believes that some of the definitions contained in the convention warrant update. Indeed, in 2015 the Lanzarote Committee issued an opinion recommending that states should extend the crime of grooming for sexual purposes to ensure it also includes "cases when the sexual abuse is not the result of a meeting in person, but is committed online",[17] that is, beyond circumstances where a physical meeting occurs. Section 474.27 of the Australian Commonwealth Criminal Code Act criminalises the grooming of children under 16 for the purpose of sexual activity,[18] in line with the Lanzarote Convention. However, the provision does not explicitly clarify that "the sexual activity" may occur entirely via technology, leaving this open to defence. The legislation also does not protect children between 16-18 years of age from grooming.

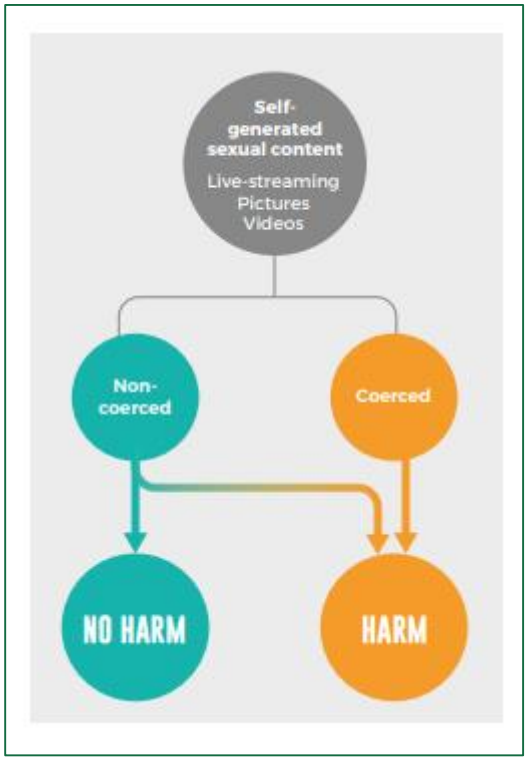
Live-streaming of child sexual abuse

Live-streaming tools can be used to transmit sexual abuse of children instantaneously to one or more viewers, so that they can watch it while it is taking place. Remote viewers may even be able to request and direct the abuse, and financial transactions can occur alongside it or even within the same platforms. Concerningly, for law enforcement authorities, many streaming platforms do not retain records of content shared by default and/or design, meaning it cannot be used as evidence in the event of a crime. This increases the chances of impunity for offenders, and creates specific challenges for investigators, prosecutors and courts.

A rise in the 'sharing of self-generated sexual content involving children' has been noted in different contexts and by a range of global actors.[19,20] But this is a complex issue and includes a range of different experiences, risks and harms. Some self-generated content is created and shared by adolescents voluntarily and such exchanges may be increasingly becoming part of young people's sexual development. In some instances young people have expressed that that it may provide advantages in their relationships and increase their self-esteem.[21] However, the creation and sharing

[16]INTERPOL. (2020). Threats and trends. Child sexual exploitation and abuse. COVID-19 Impact. 7.
[17] Council of Europe's Lanzarote Committee. (2015). Opinion on Article 23 of the Lanzarote Convention and its explanatory note. Para 20.
[18] Government of Australia. (1995). Criminal Code Act 1995. Section 474.27.
[19] EUROPOL. (2020, June). Exploiting Isolation: Offenders and victims of online child sexual abuse during the COVID-19 pandemic.
[20] Thorn & Benson Strategy Group (2020). Self-Generated Child Sexual Abuse Material: Attitudes and Experiences.
[21] ECPAT Sweden. (2020, May). "I början vart det lite läskigt men nu är det vardag" En rapport om yngre barn och egenproducerat material.

of self-generated sexual content can be coerced, for example through grooming, threats or peer-pressure. While coercion can clearly be seen as a crime and leads directly to harm, there can be negative consequences for children sharing any sexual content including in cases where sharing is not coerced. Material shared voluntarily may not cause harm at first, but there remain risks if it is later shared beyond the control of the person who created it. Once it exists, such content can also be obtained deceptively or by using coercion, and circulated by offenders perpetually.



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.

How to enable faster investigations that can better respond to rapidly evolving trends in offending and role of technology companies

(Response to point c and e of the inquiry)

Robust legal frameworks, while extremely important, are not sufficient by themselves to address online child sexual exploitation. Effective policing of these crimes requires, in the first place, specific expertise in information and communication technologies 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.

The ECPAT Summary Papers on Online Child Sexual Exploitation and on Sexual Exploitation of Children in Travel and Tourism, published in 2020, identified a few relevant recommendations and ways forward to better respond to the ever-changing nature of online child sexual exploitation.

Firstly, States should enhance international cooperation and international investigative coordination. For borderless crime, a borderless response is necessary. International collaboration plays a vital role in improving the effectiveness of national law enforcement agencies by creating more efficient operational activities where police units can join forces, avoid duplication, and build regional capacities. Australian law enforcement is already recognised as a leader in this sphere, and this work should continue and expand, particularly with regional neighbours in the Pacific and Southeast Asia.

Considering ways to impose legal responsibilities that encourage smooth collaboration with online service providers to promptly comply with law enforcement requests for information, including across borders, to retain data for a minimal period, and to filter and/or block and/or take down child sexual abuse material. This will assist with the investigation of crimes as well as in controlling the wide distribution of child sexual abuse material.

Finally, legal responsibilities on electronic/online service providers may be considered that require demonstrable efforts to minimize children's experiences of online child sexual exploitation and abuse on their platforms – safety first approaches. These may impose liability on platforms where sexual exploitation has been facilitated.

Use by offenders of encryption, encryption devices and anonymising technologies

(Response to point d of the inquiry)

A key concern impacting children's safety is the widespread adoption of end-to-end encryption (E2EE) by tech platforms, in particular instant messenger services. Many cite legitimate privacy concerns from users of their platforms as a reason,[22] and major tech companies have identified this method as the best solution to address privacy concerns.[23] However, E2EE also provides perpetrators of online child sexual exploitation, whether they are sharing images or communicating for sexual purposes with a child, with privacy and in some cases anonymity to carry out these offences. Many technology platforms have provided encrypted services[24] and any child protection agencies have vocally criticised encryption plans, highlighting that this move would pose serious challenges for investigations and prosecutions, enabling perpetrators to act anonymously and stopping the ability of providers to proactively detect millions of instances of child sexual abuse material on their platforms[25] will also considerably limit the ability of law enforcement to detect suspicious behaviours towards children and collect evidence, including by preventing the use of effective tools used for the detection and removal of known child sexual abuse material from platforms.[26]

---

[22] 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

[23] *Ibid*.

[24] Mark Zuckerberg. (2019). A privacy focused vision for social networking.

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

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

Considering that over 50% of Internet traffic is already encrypted,[27] companies have an obligation to invest in the development and deployment of systems and tools that can aid investigations and detection of child sexual abuse material and other harmful behaviours in their end-to-end encrypted platforms that are as efficient as systems relying on content detection operating in non-encrypted environments.[28] A recent announcement by Apple has demonstrated categorically that this is possible.[29]

Therefore, to ensure that law enforcement is capable of investigating child exploitation cases, online service providers must not be allowed to prioritize the privacy of all users through E2EE over the right to protection for all children and indeed the right to privacy for victims of online child sexual exploitation and abuse. They must be held accountable for the services they are providing and the known negative impact they have on children. For this reason, any changes to Australian legislation must establish rules for accountability and transparency, and ensure a liability regime that is enforced through appropriate audit and inspection measures. Companies should also be encouraged or required to adhere to safety-by-design principles. Companies should only retain immunity from liability if they can demonstrate they have taken all reasonable and proportionate steps to anticipate and mitigate to the greatest extent possible the potential for their platform or services to be misused in ways which harm children.

To conclude, ECPAT International would like to highlight that end-to-end encryption without safeguards and liability regimes for companies will enable the continuation and probably expansion of child sexual abuse exploitation and make the work of law enforcement even harder.[30]

[27] *Ibid.*
[28] ECPAT International. (2020). Summary paper on online child sexual exploitation. 15.
[29] Apple. (n.d.) Expanded Protections for Children.
[30] ECPAT International. End-to-end encryption.