1. **Introduction**

This submission by [ECPAT International](https://www.ecpat.org/)[[1]](#footnote-1) is in response to the call issued by the Committee on the Rights of the Child regarding its upcoming General Comment on children’s rights in relation to the digital environment. Acknowledging that the focus of the General Comment will be placed on different groups of children’s rights in the digital world, ECPAT’s contribution specifically focuses on the protection of children from the risks and harm of online child sexual exploitation (OCSE).[[2]](#footnote-2)

 ECPAT’s submission examines what is currently known about the scale and scope of OCSE and explores the main challenges and focus areas for addressing related global evolving harm and risks. Furthermore, it provides related examples of reported good practices in line with the WeProtect Global Alliance [Model National Response](https://static1.squarespace.com/static/5630f48de4b00a75476ecf0a/t/582ba50bc534a51764e8a4ec/1549388168335/WePROTECT%2BGlobal%2BAlliance%2BModel%2BNational%2BResponse%2BGuidance.pdf), a policy model which aims at looking at solutions from a comprehensive perspective across sectors. This submission is based on previous research conducted by ECPAT International and incorporates contributions made by members of the ECPAT Network for the purpose of this call.

**OCSE as a fast evolving global threat**

Over the last 20 years, as the world rapidly became inter-connected through technology, children have been increasingly exposed to evolving risks online and some fell victims of harm through the misuse of technologies. The presence of millions of children active online, has made it easier for offenders to contact victims. Additionally, advances in technology enables perpetrators to use tools such as anonymous platforms, streaming services, encrypted communication systems and virtual currency, allowing them to easily share materials and communicate with each other through online communities.[[3]](#footnote-3)

These developments have expanded the notion of OCSE to include not only the production, possession and distribution of child sexual abuse/exploitation material (CSAM/CSEM) but also related practices such as live streaming of child sexual abuse, sexual extortion and coercion online and grooming, among others.[[4]](#footnote-4) Besides increasing children’s vulnerability online, the rapid evolution of new technologies also poses a challenge for law enforcement, researchers and advocates who often find themselves outpaced as they try to combat the ever-changing criminal threats.[[5]](#footnote-5)

1. **Finding solutions: a review of good practices to fight OCSE.**

The global and complex nature of the problem requires national and international responses in which governments, NGOs and the private sector cooperate to address the challenge of children online safety and disrupt the dynamics of OCSE. ECPAT International advocates on the necessity of a coordinated response to this threat and promotes initiatives such as the WePROTECT Global Alliance [Model National Response](https://static1.squarespace.com/static/5630f48de4b00a75476ecf0a/t/582ba50bc534a51764e8a4ec/1549388168335/WePROTECT%2BGlobal%2BAlliance%2BModel%2BNational%2BResponse%2BGuidance.pdf), which provides a policy framework to develop cross-sector capabilities at the national and international levels to end child sexual exploitation and abuse. After consultation with our Network members, ECPAT International aims to use this submission to outline some examples of good practices in the six key areas identified in the Model National Response: Policy and Governance; Criminal Justice; Victims; Society; Industry; and Media and Communications.

The examples below include examples of successful programmes conducted by ECPAT International and ECPAT Network members in the recent years as well as new policy initiatives and legislation adopted by national governments to protect children from OCSE.

* 1. **Policy and governance: improving domestic legislation and promoting national and international research on OCSE.**

Comprehensive legislation on OCSE is an essential step for States to mitigate risks and protect victims in line with their commitments to the Convention on the Rights of the Child. Some countries have done so by updating their domestic legislation to include new crimes reflecting the current reality of OCSE and its many manifestations. For instance, Peru updated its Criminal Code in 2018 to include the criminal conducts of online sexual harassment, grooming and online sexual extortion.[[6]](#footnote-6) Similarly, Malaysia enacted the Sexual Offences Against Children Act in 2017, which criminalises conducts related to CSAM/CSEM and online grooming.[[7]](#footnote-7) Additionally, Taiwan made amendments to the Youth Sexual Exploitation Prevention Act in 2015 to update the definition of child sexual exploitation, formally recognising OCSE.[[8]](#footnote-8)

At the international level, ECPAT International advocates for better domestic legislation to ensure that countries have laws that are in line with internationally agreed conventions. In recent years, ECPAT’s country reports, as well as reports to the UN Human Rights Council and the CRC Committee have been instrumental in helping governments identify gaps in the law so they can make appropriate changes. To this effect, we have also developed a [global database](https://globaldatabase.ecpat.org/) mapping the different national legal frameworks protecting children from OCSE.

Besides a comprehensive legal framework, national and international research on the topic is needed to inform an authoritative view of the threat, trends and current responses to the problem and enable the development of effective policies.[[9]](#footnote-9) Despite the scope and significance of OCSE globally, there is widespread recognition of the scarcity of reliable data on the topic. The clandestine and criminal nature of the phenomenon as well as methodological, ethical and legal challenges and highly limited resourcing by governments and other institutions significantly constrain evidence generation in this domain.[[10]](#footnote-10) The lack of quality research hampers decision-makers’ ability to grasp the true nature and scope of this widespread form of child sexual exploitation and can even lead to the adoption of ineffective or counterproductive policies.

ECPAT International is committed to address this gap and contribute to global research on OCSE by placing evidence generation among its strategic goals.[[11]](#footnote-11) In March 2018, ECPAT and INTERPOL co-launched the flagship research report “[Towards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material](https://www.ecpat.org/wp-content/uploads/2018/02/Technical-Report-TOWARDS-A-GLOBAL-INDICATOR-ON-UNIDENTIFIED-VICTIMS-IN-CHILD-SEXUAL-EXPLOITATION-MATERIAL.pdf)”. The research included analysis of a sample of images and videos housed at INTERPOL in its [INTERPOL International Child Sexual Exploitation database](https://www.interpol.int/en/How-we-work/Databases/International-Child-Sexual-Exploitation-database) (ICSE Database), which is an investigative tool containing CSAM/CSEM seized by law enforcement around the globe and used as evidence in criminal enquiries. This report provides qualitative and quantitative data on the level of victimisation, profile of victims and offenders portrayed on CSAM/CSEM. Interesting findings include links between the age and gender of the victim and the severity of abuse; when victims were younger, the abuse was more likely to be extreme. Similarly, videos and images featuring boys were more likely to show severe abuse.[[12]](#footnote-12)

At the national level, the [Child Rights Center Albania/ECPAT Albania](https://www.crca.al/sq) published in 2019 the first ever report on online child and youth safety in the country, which included the analysis of data collected by the National Platform for Child Internet Safety.[[13]](#footnote-13) Other examples of good practices include research commissioned by the Ministry of Justice and Security of the Netherlands, which focuses on the phenomenon of sexting and its causes.[[14]](#footnote-14)

* 1. **Criminal Justice: capacity building and international cooperation for effective and successful OCSE investigations.**

In order to ensure an effective response to the threats of OCSE, law enforcement agencies need to be equipped with the knowledge, skills, tools and resources required to conduct investigations, prosecute offenders and protect victims. States need to allocate enough resources to ensure the specialisation of law enforcement officials so they can keep up with the ever-changing threats and *modus operandi* of online offenders. As an example, Albania recently approved a National Action Plan on Safer Internet for Children, including programmes for the specialisation of staff through manuals and trainings on OCSE case management.[[15]](#footnote-15)

Furthermore, cross-sector cooperation between stakeholders is also key since, in many occasions, civil society organizations and the private sector are sufficiently equipped to provide law enforcement or the justice system operators with technical assistance and specialized knowledge on specific issues. In Taiwan, the Ministry of Justice has worked with [ECPAT Taiwan](https://www.ecpat.org.tw/) over the past decade to carry out trainings for the police and prosecutors on identifying and investigating OCSE cases on a yearly basis.[[16]](#footnote-16)

Not only cross-sector cooperation, but also international cooperation between law enforcement in different countries is essential to address the global nature of the threat. One of the main challenges is that new technologies not only facilitate opportunities for perpetrators to contact victims worldwide but also enable increasing amounts of CSAM/CSEM to be shared globally.[[17]](#footnote-17) CSAM/CSEM distribution is multi-jurisdictional, which means that an offender and his/her victims can be located in different jurisdictions. In this sense, international cooperation of law enforcement agencies to share information and intelligence is essential to enhance effective prosecution of offenders, a speedy victim identification and rescue process and avoid duplicated investigations.

One global tool that aims to facilitate international cooperation between law enforcement agencies is the aforementioned ICSE Database.[[18]](#footnote-18) It was launched in 2009 and is used by certified law enforcement officers and others, to investigate CSAM/CSEM in the form of images, videos or hashes and compare them to other such data seized by law enforcement worldwide and stored in the database. There are currently more than 55 countries connected and contributing to the database, as well as INTERPOL and Europol staff. By January 2017, INTERPOL reported that 10.000 sexual abuse victims had been identified by the member countries in the last seven years.[[19]](#footnote-19) While these numbers are far from insignificant, global identification capacity would be greatly improved if more countries were connected to this global database. Following the release of the flagship research report co-launched with INTERPOL, ECPAT International has been raising awareness about the role of the ICSE Database in enhancing CSAM/CSEM victim’s identification efforts at country-level through regional advocacy events held in 2018. After this, ECPAT international has continued working with INTERPOL and other stakeholders in encouraging greater participation by countries not yet connected.

* 1. **Victims: appropriate support services and child helplines to ensure a victim-centered approach.**

Appropriate support services for OCSE victims as well as accessible reporting mechanisms such as hotlines and child helplines are essential to enable the intervention of law enforcement and child protection services and to ensure that the needs and rights of child victims are prioritised during investigations.

Several members of the ECPAT Network carry out victim support programmes in their respective countries providing child victims of OCSE with integrated and personal assistance and covering the gaps of national support services. [CHS Alternativo](http://www.chsalternativo.org/), the ECPAT member in Peru, provides psychological support, legal assistance and covers the immediate basic needs of victims such as shelter, transport and personal hygiene as well as medium and long-term assistance for the purpose of reinsertion by facilitating financial support for education fees or professional training. CHS Alternativo has also developed technical assistance and workshops to strengthen the capabilities of child protection professionals. Workshops have focused on psychological attention for victims, understanding of grooming processes as well as legal assistance for cases dealing the new OCSE-related crimes added to the Criminal Code in 2018 (online sexual harassment, grooming and online sexual extortion).

Other initiatives include services such as confidential child helplines offering psychological support and consultation, as well as referrals. These helplines are an effective reporting and prevention mechanism for children at risk and child victims of sexual exploitation. Moreover, child helplines and hotlines are effective data collection tools for researching forms of OCSE; allowing organizations to highlight emerging trends and gaps in child protection. The [Jordan River Foundation](http://www.jordanriver.jo/) (JFR), the ECPAT member in Jordan, who manages one of these helplines, reported that in 2018, 36 cases of online sexual abuse were received through the helpline. Interestingly in all the cases, the perpetrator was someone known to the child, either neighbours, partners or people in their social circle confirming findings from similar research.[[20]](#footnote-20)

* 1. **Society: Informing parents of risks and empowering children to protect themselves from OCSE.**

One of the biggest challenges presented by OCSE is the lack of awareness about risks online among parents, teachers and childcare professionals. Very often, this digital gap implies that young children have a more sophisticated understanding of the Internet than their parents do. This means that caregivers can many times be unprepared to teach them about online safety tools and warn them about potential risks.[[21]](#footnote-21) Furthermore, taboos surrounding sexual violence and willingness to evade parental oversight may difficult communication between adults and children, increasing the risks of OCSE remaining unreported.[[22]](#footnote-22)

Awareness raising programmes that target parents, teachers and childcare professionals on the dangers of OCSE, form a key component of the duties of ECPAT’s members at a national level. The Child Online Safety Section of [ECPAT Taiwan](https://www.ecpat.org.tw/) carried out more than 100 online safety activities at schools as well as live-streaming courses for families and children across Taiwan in 2018. Also in 2018, [Children Not for Abuse](https://www.facebook.com/ChildrenNotForAbuse/), the ECPAT member in Belarus, organized together with the IOM a model of preventive activities in rural schools to fight child abuse in cyberspace targeting children, parents and professionals working with children and developed two practical manuals on this issue for teachers and childcare professionals.[[23]](#footnote-23) Similarly, [JFR](http://www.jordanriver.jo/) reported that in collaboration with other internal bodies that work in the cybercrime field, 60 children and parents were targeted through awareness sessions related to child online exploitation in the first quarter of 2019. Based on these sessions some cases ended up being transferred to the child protection services as victims of OCSE.

An alternative approach is to focus on the agency of children, to increase their knowledge and empower them to protect themselves and their peers from online violence. The ECPAT Network has reported several examples of good practices in this regard, mostly in the form of mentoring programmes based on the peer-to-peer principle. ECPAT members in [Netherlands](https://www.defenceforchildren.nl/wat-doen-we/themas/seksuele-uitbuiting), [Germany](https://ecpat.de/), [Austria](https://www.ecpat.at/), [Belgium](https://ecpat.be/en/) and the [UK](https://www.ecpat.org.uk/) have been running since 2013 the [*Make-IT Safe*](http://www.make-it-safe.net/index.php/en/) project, a peer-to-peer mentoring programme aimed at empowering young people to protect themselves and others against OCSE. ECPAT Netherlands has also developed the “[*Make-IT-Safe cluster-4 onderwijs*](https://defenceforchildren.nl/wat-doen-we/projecten/make-it-safe-voor-cluster-4-onderwijs)” project, based on the same principle but specifically focused on internet safety for youngsters with mild intellectual disabilities. Also in the European context, [ECPAT Luxembourg](http://www.ecpat.lu/)’s youth group ([ECPAT You(th) Together](http://ecpatyouth.lu/ecpat-youth-together-2/)) raises awareness among the general public and mainly among other young people organizing peer-to-peer activities and workshops on OCSE.

Another example worth mentioning is the[E-Mentores CR Model](http://ementores.org/) developed by the [Fundación PANIAMOR](https://paniamor.org/), the ECPATmember in Costa Rica. This mentoring programme integrates child online safety into a national strategy addressing digital inclusion as a way for poverty reduction and social inclusion and acts upon the need for multi-stakeholder cooperation to counter OCSE by establishing partnerships with government agencies and the private sector at the national level.

* 1. **Industry: regulating the private sector and building partnerships for effective cooperation.**

The global nature of OCSE-related threats as well as the rapid development of information and communication technologies (ICTs) make engagement with private companies essential in the quest for solutions to the problem of OCSE. Private sector actors – especially those working in the ICT field– play a key role in not only facilitating, enabling and propagating the sexual exploitation of children through the misuse of their online platforms, systems and services but also in developing systems and platforms that can help detect and take down illegal content disrupting the dissemination of CSAM/CSEM.

Although some examples of self-regulation by these companies are promising, governments must enact legislation requiring specific actions from private sector actors and hold them accountable when their platforms or services are misused. In this sense, governments should require Internet providers to set up takedown procedures to block access and enable the removal of CSAM/CSEM from their platforms and services.[[24]](#footnote-24) So far, few countries have specific legislation covering this requirement. One example is the [Law on Cybersecurity](https://www.allens.com.au/pubs/pdf/priv/cupriv22jun18.pdf) recently passed by the Vietnamese government that obliges Internet providers to prevent the sharing and delete any contents that harm or prejudice children and to notify and cooperate promptly with the competent authorities.[[25]](#footnote-25) The law also includes provisions obliging agencies, organizations, parents, teachers, childcare providers and others to protect children in cyberspace. Although the aforementioned provisions imply an increase in child protection, the law regulates other aspects of cybersecurity that should be critically assessed. Concerns raised refer to provisions requiring providers to also remove content that the Vietnamese authorities deem to be anti-state or anti-government and criminalizing the authors of such content. This has led to harsh criticism from human rights organizations that fear a significant cutback in terms of freedom of expression and press freedom in the country.[[26]](#footnote-26)

Another key priority is the establishment of CSAM/CSEM reporting portals that enable the transmission of content to law enforcement. ECPAT International has collaborated with the [Internet Watch Foundation](https://www.iwf.org.uk/) (IWF), with the support of our member organizations to advocate for setting up reporting portals on CSAM/CSEM in African countries. Starting in January 2018, this collaboration has led to the establishment of reporting portals in Malawi, Angola and Burundi and further collaboration is aiming for the launching of portals in Rwanda, Liberia, Benin and Madagascar. Through the IWF portals, anonymously reported material, after being assessed by expert analysts of IWF, is removed from the Internet and added to a list of hashed images. If a previously flagged photo is uploaded in any part of the world, the information quickly reaches IWF allowing them to take it down once again.[[27]](#footnote-27)

ECPAT International also advocates for national governments to promote and allocate resources for CSAM/CSEM reporting mechanisms. In the Netherlands, since the beginning of 2019, the police and the Online Child Abuse Expertise Agency have been working on a database with hashcodes to identify CSAM/CSEM so ICT companies can use it to clean their own servers. Furthermore, in 2018 the Minister of Justice and Security awarded the police extra funds for the construction of a *crawler* specifically aimed at the dark web.[[28]](#footnote-28)

Another example of good practice that aims to further engage the private sector in the reporting process is [jugendschutz.net](http://www.jugendschutz.net/en/how-we-work/), a German organization that works with Internet providers by putting them on notice in case of violations, asking for illegal content removal and providing them with advice for improvements in their child protection measures.[[29]](#footnote-29)

Effective protection of children online depends on joint efforts of government bodies, international partners and the private sector. In this sense, on top of regulating the industry, governments and civil society must build partnerships in order to help businesses appreciate their digital impact on children’s rights, bring them to the policy table and work together to develop innovative solutions to the problem. An example of multi-stakeholder cooperation in this regard is the National Child Online Safety Task Force (COST) of Tanzania, which brings together policy and decision makers, law enforcement, the judiciary, mobile network operators, academics and civil society to advocate for children online safety and to ensure that any content violating children’s rights is reported and removed.[[30]](#footnote-30)

* 1. **Media and Communications: promoting a universally agreed terminology.**

Communication is of critical importance in our efforts to respect, protect and implement the rights of the child. The use of universally agreed terminology is essential to enable information and ideas to be communicated rapidly and legibly amongst all stakeholders and to ensure a victim-centered approach in the global fight to eradicate OCSE. The lack of common terminology can generate inaccuracy and inconsistency in policymaking and legislation, undermine advocacy efforts due to miscommunication, lead to imprecise research and hinder international cooperation in investigations and prosecutions. To address this problem, in 2016 [Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse](https://www.ecpat.org/wp-content/uploads/2016/12/Terminology-guidelines_ENG.pdf) were launched, aiming to help those working in the field to navigate the complex lexicon of terms that relate to the sexual exploitation and abuse of children.

1. ECPAT International is a global network of civil society organizations, working to eradicate all forms of sexual exploitation of children. Over the past 29 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 109 member organizations operating in 96 countries around the world. [↑](#footnote-ref-1)
2. Online child sexual exploitation is defined 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 Internet-related technologies that result 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. ECPAT International. (2016). [Terminology Guidelines for the Protection of Children from Sexual Exploitation and Abuse](http://luxembourgguidelines.org/english-version/), 27. [↑](#footnote-ref-2)
3. ECPAT International (2017), [Briefing Paper: Emerging global threats related to the online sexual exploitation of children](https://www.ecpat.org/wp-content/uploads/2016/05/Emerging-Issues-and-Global-Threats-Children-online-2017.pdf). [↑](#footnote-ref-3)
4. *Ibid.* [↑](#footnote-ref-4)
5. ECPAT International (2018), [Trends in online sexual abuse material](https://www.ecpat.org/wp-content/uploads/2018/07/ECPAT-International-Report-Trends-in-Online-Child-Sexual-Abuse-Material-2018.pdf), 6. [↑](#footnote-ref-5)
6. Communication from ECPAT member in Peru, [Capital Humano y Social Alternativo](http://www.chsalternativo.org/) (CHS Alternativo). [↑](#footnote-ref-6)
7. Communication from ECPAT member in Malaysia, [Protect and Save the Children](https://www.psthechildren.org.my/). [↑](#footnote-ref-7)
8. Communication from [ECPAT Taiwan](https://www.ecpat.org.tw/). [↑](#footnote-ref-8)
9. WePROTECT Global Alliance (2016), [Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response](https://static1.squarespace.com/static/5630f48de4b00a75476ecf0a/t/582ba50bc534a51764e8a4ec/1549388168335/WePROTECT%2BGlobal%2BAlliance%2BModel%2BNational%2BResponse%2BGuidance.pdf), 5. [↑](#footnote-ref-9)
10. ECPAT International and INTERPOL (2018), [Towards a global indicator on unidentified victims of child sexual exploitation – Technical Report](https://www.ecpat.org/wp-content/uploads/2018/02/Technical-Report-TOWARDS-A-GLOBAL-INDICATOR-ON-UNIDENTIFIED-VICTIMS-IN-CHILD-SEXUAL-EXPLOITATION-MATERIAL.pdf), 1. [↑](#footnote-ref-10)
11. ECPAT International (2018) [ECPAT International Strategic Framework 2018-2021](https://www.ecpat.org/wp-content/uploads/2018/07/ECPAT-STRATEGIC-FRAMEWORK-2018-2021-ENGLISH.pdf). [↑](#footnote-ref-11)
12. ECPAT International and INTERPOL (2018), [Towards a global indicator on unidentified victims of child sexual exploitation – Technical Report](https://www.ecpat.org/wp-content/uploads/2018/02/Technical-Report-TOWARDS-A-GLOBAL-INDICATOR-ON-UNIDENTIFIED-VICTIMS-IN-CHILD-SEXUAL-EXPLOITATION-MATERIAL.pdf), 43. [↑](#footnote-ref-12)
13. Hazizaj A. (2019). 1st National Report on Online Safety of Children and Young People in Albania,

CRCA Albania. [↑](#footnote-ref-13)
14. Communication from [ECPAT Netherlands](https://www.defenceforchildren.nl/wat-doen-we/themas/seksuele-uitbuiting). [↑](#footnote-ref-14)
15. Communication from ECPAT member in Albania, [Child Rights Center Albania/ECPAT Albania](https://www.crca.al/sq). [↑](#footnote-ref-15)
16. Communication from [ECPAT Taiwan](https://www.ecpat.org.tw/). [↑](#footnote-ref-16)
17. ECPAT International and INTERPOL (2018), [Towards a global indicator on unidentified victims of child sexual exploitation – Technical Report](https://www.ecpat.org/wp-content/uploads/2018/02/Technical-Report-TOWARDS-A-GLOBAL-INDICATOR-ON-UNIDENTIFIED-VICTIMS-IN-CHILD-SEXUAL-EXPLOITATION-MATERIAL.pdf), 12. [↑](#footnote-ref-17)
18. INTERPOL (n.d.), [INTERPOL International Child Sexual Exploitation database](https://www.interpol.int/en/How-we-work/Databases/International-Child-Sexual-Exploitation-database). [↑](#footnote-ref-18)
19. INTERPOL (2011, Jan 9), [ICSE Database identifies 10,000th victim of child sexual abuse](https://www.youtube.com/watch?v=Qm4Rq82OOSI) [video file]. [↑](#footnote-ref-19)
20. Communication from ECPAT member in Jordan, [The Jordan River Foundation](http://www.jordanriver.jo/) (JRF). [↑](#footnote-ref-20)
21. Livingstone, S., Haddon, L., Görzig, A. and Ólafsson, K. (2011) [Risks and safety on the internet: The perspective of European children](http://eprints.lse.ac.uk/33731/1/Risks%20and%20safety%20on%20the%20internet%28lsero%29.pdf), 28. [↑](#footnote-ref-21)
22. *Ibid.,*103-104. [↑](#footnote-ref-22)
23. Communication from ECPAT member in Belarus, [Children Not for Abuse](https://www.facebook.com/ChildrenNotForAbuse/). [↑](#footnote-ref-23)
24. WePROTECT Global Alliance (2016), [Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response](https://static1.squarespace.com/static/5630f48de4b00a75476ecf0a/t/582ba50bc534a51764e8a4ec/1549388168335/WePROTECT%2BGlobal%2BAlliance%2BModel%2BNational%2BResponse%2BGuidance.pdf), 30. [↑](#footnote-ref-24)
25. Communication from ECPAT member in Vietnam, [Vietnam Association for Protection of Child’s Rights (VACR).](https://www.ecpat.org/members/vietnam-association-protection-childs-rights-vacr/) [↑](#footnote-ref-25)
26. HRW (Dec 20, 2018) [Vietnam: Big Brother Is Watching Everyone](https://www.hrw.org/news/2018/12/20/vietnam-big-brother-watching-everyone); CNN (Jan 2, 2019) ['Stalinist' Vietnamese cybersecurity law takes effect, worrying rights groups and online campaigners](https://edition.cnn.com/2019/01/02/asia/vietnam-cybersecurity-bill-intl/index.html). [↑](#footnote-ref-26)
27. IWF – [Our International Reporting Portals](https://www.iwf.org.uk/what-we-do/how-we-assess-and-remove-content/our-international-reporting-portals). [↑](#footnote-ref-27)
28. Communication from [ECPAT Netherlands](https://www.defenceforchildren.nl/wat-doen-we/themas/seksuele-uitbuiting). [↑](#footnote-ref-28)
29. Communication from [ECPAT Deutschland](https://ecpat.de/). [↑](#footnote-ref-29)
30. Communication from ECPAT members in Tanzania, [C-Sema](http://sematanzania.org/) and [KIWOHEDE](http://www.kiwohede.org/). [↑](#footnote-ref-30)