Mechanisms for collective action to prevent and combat online child sexual exploitation and abuse

A comparative review

www.coe.int/children

Building a Europe
for and with children

End Violence Against Children
THE FUND

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Cover, layout and Illustration: DiARK
Cover Photo: © Shutterstock

Council of Europe Publishing F-67075 Strasbourg Cedex http://book.coe.int
Edited by Naomi Trewinnard

Printed at the Council of Europe

Mechanisms for collective action to prevent and combat online child sexual exploitation and abuse

A comparative review

Report prepared by John Carr, Independent Expert

Council of Europe

Contents

Table of Abbreviations

ATSA	Association for the treatment of sexual abusers
BUDAPEST CONVENTION	Council of Europe Convention on Cybercrime
CAHENF	Ad hoc Committee for the Rights of the Child
CSAM	Child sexual abuse material
CSEA	Child Sexual Exploitation and Abuse
DNS	Domain name system
DOH	"DNS over https"
EUROPOL	European Police Office
FOSI	Family online safety Institute
FOSI GRID	FOSI Global resource and information Directory
ICANN	Internet corporation for assigned names and numbers
ICSE	Child exploitation database
IETF	Internet engineering Task Force
INHOPE	International association of internet hotlines
INTERPOL	International criminal police Organisation
ISPCAN	International society for the prevention of child abuse and neglect
ISPS	Internet Service Providers
IWF	United Kingdom's Internet Watch Foundation
LANZAROTE COMMITTEE	Committee of the Parties to the Convention for the Protection of Children from Sexual Exploitation and Sexual Abuse
LANZAROTE CONVENTION	Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse
NCMEC	National center for missing and exploited children
OCSEA	Online child sexual exploitation and abuse
SDGS	United Nations' sustainable development goals
SID	"Safer Internet Day"
UNCRC	United Nations Convention on the rights of the child
VGT	Virtual global Taskforce
WEPROTECT	WePROTECT Global Alliance

Acknowledgements

This report has been prepared in the context of the Council of Europe project End Online Child Sexual Exploitation and Abuse @Europe (EndOCSEA@Europe). This project benefits all Council of Europe member states with a focus on ten countries, namely: Albania, Armenia, Azerbaijan, Bosnia and Herzegovina, Georgia, Republic of Moldova, Montenegro, Serbia, Turkey and Ukraine.

With thanks to John Carr, OBE, International Advisor on Children's Internet Safety and Security, who authored this report and to Fred Langford, Deputy CEO of the Internet Watch Foundation and President of INHOPE for his comments and feedback.

The Council of Europe gratefully acknowledges the financial support provided for this project by the Fund to End Violence Against Children.

Executive Summary

The aim of this review is to identify and analyse existing mechanisms for collective action to prevent and combat Online Child Sexual Exploitation and Abuse (OCSEA) at international and pan-European level. The Lanzarote and Budapest Conventions provide a comprehensive framework to prevent and combat this crime, including substantive and procedural criminal law benchmarks as well as preventive and protective measures to be put in place. The WePROTECT Model National Response also provides valuable guidance for policy makers.

OCSEA does not respect national jurisdictions. The internet has facilitated access to children of all ages in any and every jurisdiction for child sex offenders. It has provided a space where perpetrators can exchange Child Sexual Abuse Material (CSAM) and increase their knowledge of techniques to offend. Communities of offenders have formed, which has had the effect of decreasing social inhibitions, potentially spurring additional or more extreme offences. The actors necessary to fight this crime include a broad range of stakeholders. No single State or group of non-State organisations can fight this crime alone. Co-operation and mutual-assistance at international and pan-European levels are therefore absolutely essential to respond effectively. Only through multi-disciplinary co-operation at national and international levels is it possible to identify, locate and safeguard victims and effectively prevent, investigate and prosecute these types of crimes against children. Such co-operation must have the ability to respond rapidly to changes in technology and to offending behaviours.

To this day, hotlines and the associated law enforcement machinery for investigating offenders and identifying victims stand out as the only concrete examples of on-going operational mechanisms for collective action by both state and non-state actors in relation to combatting OCSEA at international and pan-European levels.

More details on hotlines are provided below however, as this report will show, there are many other vehicles which foster co-operation, collaboration, the exchange of information or provide advice on issues connected with OCSEA, even if none quite mirror or match the substantial arrangements developed to deal with images and the identification of victims.

This is merely a reflection of the fact that, for practical purposes, it is simply impossible to work on images and victim identification without international co-operation given the transnational nature of the internet. Whereas in other areas of child welfare and child rights online there is not the same urgent operational or day to day imperative to collaborate given that the children's workforce tends to be defined by, is required to work and be accountable within, nationally defined professional and legal standards. There appears to have been few political or other incentives to harmonise these standards across jurisdictions and even if that obstacle were to be overcome there are limited capacities to bring about the harmonisation such a development would imply.

Introduction

In the early to mid-1990s the sudden availability of CSAM on an unprecedented scale provided the first evidence that the internet was going to create new types of risk to children. The continued circulation of large volumes of CSAM on the internet is a very long way from being solved although, as this report will show, recent technological developments are showing considerable promise.

Each image, video or stream of a child being sexually abused is an image of a child in need of help both to recover from the psychological and possibly physical harm caused by the original act of sexual abuse depicted, but also from the additional harm caused by the publication and distribution of the material.

The continued circulation of CSAM of an individual child not only represents an infringement of that child's right to privacy and human dignity, it also puts the child at risk of further sexual abuse and other harms. This puts a major premium on victim identification and safeguarding but in addition, to the extent that the on-going circulation of CSAM encourages new and existing paedophile activity, it represents a threat to children as yet unharmed in every country of the world. For these reasons there continues to be a major focus on addressing CSAM on the internet.

No one knows how much CSAM is circulating on the internet today or how much was circulating yesterday. Neither can we know or make any confident predictions about how much is likely to be circulating on the internet tomorrow. The only thing we can be certain of is that the numbers are vast.

While it is possible to spot trends and changes in behaviour in respect of CSAM, at least in the short term evidenced by changes in the nature of the content of the images being reported to hotlines and law enforcement, it is not enough to simply observe such changes. National or global threat assessments by their very nature reflect historic data and can only make educated projections.[1]

If a greater number of cases are being reported, is that simply a sign that more people know what to do if they find CSAM or is it an indication that more CSAM is being produced and distributed? If new forms of abuse are observed, is that the beginning of a new and widespread long-term problem or is it localised and temporary? Nobody has any way of answering such questions with any degree of certainty.

Self-regulation

When the internet first started to emerge as a mass consumer technology there was a limited understanding within and around most governments and inter-governmental institutions, including law enforcement agencies, of the power and potential of the technology, or indeed of how it actually worked even at a very basic level.

In respect of egregious criminal acts, including the hosting or distribution of CSAM, internet companies

[1] See WePROTECT (2018) Global Threat Assessment, OGL, London

appeared willing to co-operate with the police in order to remove it from their services and help determine who had put it there. Sometimes this was done without there always being an obvious legal basis for that co-operation, although eventually such legal bases were put in place in most countries. Nevertheless, this willingness to co-operate was a good augury and it helped make the idea of "self-regulation" attractive.

The right for technology companies to innovate was treated as sacrosanct. Innovation promised to create new economic growth, new wealth and new jobs, reducing costs while at the same time improving the speed and ease with which people and businesses could communicate with each other. Moreover, most of the wonderful new services the companies were providing to the public appeared to be "free", which in reality meant no one had to hand over any money at the point of use. Revenues would be generated in other less obvious, less immediate and less visible ways.

This dedication to the idea of letting businesses "get on with it" with minimal if any "interference" from governments or state agencies played into and strengthened the idea of self-regulation as the preferred approach for addressing any problems that technology might throw up. However, the laissez-faire approach which underpinned the self-regulatory model allowed a distinct culture to develop within the industry. As Professor Ross Anderson remarked, a typical attitude among technology businesses was "ship it Tuesday, fix it by Version 3".[2] This approach surely has no place in a world where the internet is now so pervasive and where children are known to have a large and persistent presence. One in three of all human internet users in the world are children, this rises to around one in two in many lower income countries and is around one in five in higher income nations.[3]

Self-regulation at the national level found its counterpart internationally in the emergence of multi-stakeholder institutions which ostensibly were founded on the idea that the solutions which could be developed and agreed by consensus within them would have some degree of international backing and therefore some prospect of success. However, self-regulation came with no real means of checking or confirming if the businesses that said they would self- regulate were in fact so doing. Examples of what can happen where no means of confirming that promises were being kept soon began to emerge (see below, Blackberry case study).

Companies seemed only to act speedily following calamities which attracted major, critical media attention. This suggested that, despite repeated assertions to the contrary, a concern for online safety was not deeply embedded in business culture. A company that put safety at the heart of its affairs would not have to wait for a tragedy before being seen to act urgently and effectively.

A few major technology companies still argue that self-regulation has been a successful model, but on a broader front it now appears to be accepted that a framework of laws and obligations is needed.[4] That does not mean there is no room for any kind of self-regulatory processes, but there is now a strong case for saying that these should be contained within a clear framework of legally defined and enforceable rules and expectations.

The flaws in the self-regulatory and multi-stakeholder models are now much better understood but a prolonged attachment to them seems to have retarded the development of effective mechanisms for action both at national and transnational levels.

---

[2] Anderson, Ross (2001), Why Information Security is Hard, CL.CAM, Cambridge, available at: https://www.cl.cam.ac.uk/~rja14/Papers/econ.pdf

[3] Livingstone, Sonia; Byrne, Jasmina; Carr, John (2016). One in Three: Internet Governance and Children's Rights, Innocenti Discussion Papers no. 2016-01, UNICEF Office of Research - Innocenti, Florence, available at: https://www.unicef-irc.org/publications/795-one-in-three-internet-governance-and-childrens-rights.html

[4] https://www.bbc.com/news/world-us-canada-47762091

In preparing this report it is striking how few effective, operational mechanisms exist which have the resources or capacity to work on online child protection issues outside of industry-dependent or industry-supported bodies. This is true both nationally and transnationally. One of the consequences of this is the striking inequality which exists between the resources which internet businesses can deploy to tackle OCSEA compared with those which are available to Governments, law enforcement agencies and civil society.

The case for collective action

Implied in the failure of self-regulation is the suggestion that there has been too great a reliance on the presumed openness of the industry, as expressed through their participation in multi-stakeholder environments.

Transparency is the beginning of any real potential to tackle the remaining OCSEA challenges, it lies at the heart of being able to formulate effective policies. Yet up to now internet businesses have been extremely reluctant to disclose any substantive data about their internal operations and even where such disclosures have been made, a great many state institutions have limited capacities to interpret such data.

Recently, Facebook and Google have started issuing "enhanced transparency reports". These are a welcome recognition of the growing importance of publishing more information about what is happening on internet platforms. However, insofar as these reports are limited to companies saying to parents, children, governments and the general public "this is what we think you need to know and this is what we are willing to tell you", they are not sufficient as the basis on which to proceed in the longer term.

Hitherto there have been immense practical difficulties for civil society organisations and governments to collect and exchange information with each other about effective actions and successful programmes which have been evaluated and been shown to work well.

Case Study: Blackberry

In 2005 the UK's mobile phone networks proclaimed in an industry code of practice that all mobile networks were to restrict access to CSAM and to adult content.

At the relevant time (2010/11) there were about 8 million Blackberry handsets in use in the UK. The company had a significant share (one-fifth) of the total smartphone market. It turned out that, with the exception of the 700,000 Blackberry users who were on T-Mobile's network, the other 7,300,000 Blackberry users on all the other networks were not shielded from adult content, neither were they protected from the possibility of being exposed to CSAM. This was because the Internet Watch Foundation's list of URLs for CSAM and the adult content filters used across the industry would not work on Blackberry devices unless special arrangements were made, as with T-Mobile.

This was particularly unfortunate because at that time Blackberry handsets were hugely popular with children as they had pioneered "free" messaging services. Yet for quite some time (until this lacuna was discovered by an investigative journalist) neither Blackberry themselves nor any of the networks made it clear to their existing customers or would be customer that if they used Blackberry handsets on any network other than T-Mobile, they would not benefit from the protections trumpeted by the industry code of practice.

In the absence of any mechanism to verify the claims made by the industry it was impossible for other parts of the multi-stakeholder environment, including government, to discover the truth.

This is a key reason why a major proposal of this report is to establish or commission a new Think Tank or Global Observatory to act as a focal point to develop transnational working-methods to further the rights of the child in the digital environment. Many of the businesses each government and civil society organisation deal with are the same. These businesses have a variety of mechanisms to stay abreast of developments in all parts of the world, either due to internal capacity or through trade associations. They know what works and what does not, judged by their own standards. They know what might threaten vital commercial interests and therefore needs to be resisted. Policy makers inside governments and in civil society need to develop corresponding capabilities and enhance co-operation with these businesses to transform this knowledge into binding policy obligations.

Addressing CSAM

As previously mentioned, one of the longest established areas of activity in relation to OCSEA has been in respect of CSAM.

The potential for computers and computer-based networks to be misused by persons with a sexual interest in children was first noted in the USA in the early 1980s but major police actions and prosecutions did not materialise until the mid-1990s in the form of prosecutions for the production or distribution of CSAM.[5] These cases gave the first hints that the then new technologies might be a mixed blessing for some children.

In those days the "internet industry" consisted principally of Internet Service Providers (ISPs). These were businesses providing connections to cyberspace. The court cases and attendant publicity around the early arrests prompted children's NGOs, Governments and law enforcement agencies to press ISPs to act to remove the images and pass on relevant information to the police, whose task it was to investigate the source, locate the distributors and any offenders involved in making or downloading them. Most importantly, the police were expected to identify, find and safeguard the victims.

Mechanisms to allow CSAM to be reported to initiate removal and associated processes started to be created independently in different jurisdictions. These mechanisms became known as "hotlines".[6] The first ones were established in 1995-96 in the Netherlands, Norway, Belgium and the UK.

Hotlines operate a portal to receive complaints about apparent illegal content from the public. Teams of analysts then assess the content in accordance with their national laws and, if they consider the content to be illegal, trace the material to a hosting country. If the content is illegal in the hosting country, then the national hotline takes steps to have the material 'taken down' in consultation with local law enforcement partners and in partnership with mobile network operators and internet service providers.

Several references to hotlines have already been made because of the key role they have played hitherto in the struggle to eliminate CSAM from the Internet.

The vast majority of hotlines were and remain essentially reactive in nature. This means they have to wait to receive a report concerning CSAM before they can take steps to secure its removal or report it to the police, typically by issuing a takedown notice to the host. In many jurisdictions it is a crime for anyone, no matters how well-intentioned, to seek out CSAM intentionally. Thus, not only were the hotlines obliged to

[5] Lanning, Ken (2018) Love, Bombs and Molesters, an FBI Agent's Journey, Kenneth Lanning
[6] GSMA in association with INHOPE (2013) Hotlines: Responding to reports of illegal content, UK

sit back and wait for someone to make a report to them, they were meant to sit back and wait for accidental discoveries to be reported.

A number of hotlines began to lobby for the law to be changed to allow them to start looking for CSAM proactively. In 2013 this possibility was given to the Internet Watch Foundation (IWF) and the number of images it was able to identify and remove began to climb steeply.[7] It is understood that only a handful now have similar pro-active powers, a European Union review currently underway will clarify exactly how many. It is the first time a review of this kind and scale has been undertaken. It has been prompted by a desire, on the part of the EU, to ensure they are giving the best possible support to combat online CSAM, it has also been spurred by major technical advances and changes.

However, there is a growing awareness of the need for proactivity to become the basis of future work in this area. In some jurisdictions this is presenting considerable legal challenges. For example, in Italy the hotlines are not even allowed to look at any images that are reported to them, even if only to confirm they are, in fact, CSAM.

The newly established power to search proactively was of itself an important development. However, a really dramatic change took place when the ability to work proactively was also combined with the power of hashing technologies such as PhotoDNA.[8] The Canadian hotline, working closely with the National Center for Missing and Exploited Children (NCMEC), the US hotline, pioneered this approach and the IWF has also adopted similar techniques.

The change in scale which these developments have permitted on the face of it is staggering and represents an enormous change. In the latest available Annual Report of the International Association of Internet Hotlines (INHOPE) it is recorded that in 2017 all the hotlines in membership identified 259,016 images.[9] By way of contrast or comparison, in January 2017 the Canadian hotline revealed that their "Project Arachnid" had, in an experimental period of six weeks, looked at over 230 million web pages, identifying 5.1 million unique web pages containing CSAM including 40,000 unique child sex abuse images. The project is now identifying "over 100,000 unique images per month…, and this number has been increasing each month."[10] Using similar techniques, Facebook revealed that during a three month period in 2017 it had discovered and removed 8.7 million "child nudity" images, 99% of these were detected by automated systems before anyone had reported them.[11] This meant that it is possible that they were not seen by anyone other than the individual who posted them. It is not known how many of these would qualify as CSAM but the point is clear.

The ability to remove images from the internet much more rapidly and on a significantly larger scale is extremely important both in its own right and above all, as the Phoenix 11 group have testified, it is important for the victims depicted in the images.[12] It is too soon to say if there will be any wider benefits arising from the new pro-active methods. The ability to identify, locate and arrest offenders or to identify, locate and safeguard victims depends on the availability of resources both within the law enforcement community and also within safeguarding agencies. Given how stretched their resources already are, simply having larger volumes of images to deal with is unlikely to improve matters. However, removing the images from circulation on the internet is a worthy end in and of itself. In the long run, as the efficiency of pro-active searching improves, it is likely to be the case that individuals considering using the internet to distribute material will be forced to think again and this will lead to a reduction in traffic, allowing

[7] https://www.iwf.org.uk/news/our-2015-annual-report
[8] https://www.microsoft.com/en-us/photodna
[9] http://88.208.218.79/tns/news-and-events/news/18-06-25/INHOPE_Annual_Report_2017
[10] https://www.cybertip.ca/app/en/projects-arachnid
[11] https://www.bbc.co.uk/news/technology-45967301
[12] https://protectchildren.ca/en/programs-and-initiatives/phoenix11/

relevant agencies to devote more resources to a smaller caseload. Furthermore, the emergence of pro-active searching opens up the possibility of streamlining part of the work undertaken by hotlines, which is concerned with locating CSAM and securing its removal or restricting access to it. It is unlikely that much would be gained by having a multiplicity of hotlines all using the same hashes and crawling techniques and all searching the same global internet. Avoiding duplication by developing pro-active techniques, could free up resources to focus on improving other parts of the important work that hotlines carry out.

The existence and promotion of a hotline sends a strong message to distributors or would-be distributors of CSAM: that machinery exists which will help track them down and facilitate their arrest. As such they act as a deterrent to becoming involved in such behaviour. In addition, the existence of a hotline sends a signal to children, perhaps particularly victims, that machinery exists to protect them or address their grievances, even in cyberspace.

Thus, while the case for every jurisdiction to have an adequate legal framework for addressing CSAM and for having a hotline remains strong, it also needs to be recognised that significant changes are likely to occur in the near future which will impact on the way hotlines operate.

Mechanisms for collective action to strengthen governance structures and multi-stakeholder co-operation

It is difficult to precisely pinpoint when the position of children as internet users started to register in a major way on the agendas of transnational governmental institutions. The EU began funding projects with a link to the internet under the Daphne Programme in 1997.[13] Soon afterwards it started funding newly emerging hotlines (see below) and later established the "Better Internet for Kids" initiative.[14] In 2003, the United Nations initiated the World Information Society process.[15] However, in 2011 a major turning point appears to have been reached when President Sarkozy of France used the platform of a G8 Summit to draw attention to the need for international action to protect children in online environments.[16]

As the UN Committee on the Rights of the Child recalls in General comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights:

> *"8. The present general comment principally addresses States' obligations under the Convention and the Optional Protocols thereto. At this juncture, there is no international legally binding instrument on the business sector's responsibilities vis-à-vis human rights. However, the Committee recognizes that duties and responsibilities to respect the rights of children extend in practice beyond the State and State-controlled services and institutions and apply to private actors and business enterprises. Therefore, all businesses must meet their responsibilities regarding children's rights and States must ensure they do so. In addition, business enterprises should not undermine the States' ability to meet their obligations towards children under the Convention and the Optional Protocols thereto."* [17]

Since 2011 a series of organisations and transnational initiatives have emerged which have similar agendas. These initiatives have their roots in specific political circumstances or organisational histories. This brings a risk of duplication of effort, not least in respect of fundraising, both on the part of the initiatives themselves seeking donations from sponsors and groups or organisations applying for funding for particular projects.

In addition, there is still a comparatively small number of people within different Governments, international governmental organisations, companies and NGOs who are engaged with work in this area. This means the task of following the activities of the different initiatives, getting to understand their processes, priorities and procedures can place a considerable strain on the available resources. There is the

[13] http://www.europarl.europa.eu/RegData/etudes/STUD/2019/608857/IPOL_STU(2019)608857_EN.pdf
[14] https://blogs.lse.ac.uk/mediapolicyproject/2018/05/21/the-european-strategy-for-a-better-internet-for-children
[15] https://www.itu.int/net/wsis/geneva/index.html
[16] https://www.theguardian.com/technology/2011/may/24/sarkozy-opens-e-g8-summit
[17] http://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2fPPRiCAqhKb7yhsqIkirKQZLK2M58RF%2f5F0vFwFEdvfY9OsFrg-Vu%2fCF2Thh%2feVq0BUAwrMlB0uLB65Sr6%2byVYyL3juTIKDZpGqiTDqI39zFR2e5zEyyqKwnnTD

further risk of "consultation fatigue" and, with limited travel budgets, who turns up to participate in which events can be rather random, leading to outcomes of varying quality. Moreover, there is the potential for different initiatives to develop different standards or approaches.

There is no suggestion that the existing transnational initiatives need to be pruned or merged, but the case for there being a high level of co-ordination and co-operation is self-evident, for example in relation to the timing of different events or processes. To some degree this is being achieved at the moment by virtue of the fact there are a number of individuals involved in the different processes whose membership overlaps with more than one organisation. If that were to change, there would be a strong case for formalising communications and co-ordination.

United Nations

The UN Special Representative of the Secretary General on Violence Against Children published a report on ICTs, the Internet and violence against children in 2014 to promote the empowerment of children in the online environment, highlight lessons learned and strengthen the protection of children online.[18] The Special Representative has continued engaging with governments and other stakeholders to promote the adoption of frameworks to promote the rights of the child in the digital environment and to work towards the full implementation of the UN Sustainable Development Goals (SDGs).

The UN Special Rapporteur on the sale of children, child prostitution and child pornography published a thematic report focussing specifically on Information and communication technologies and the sale and sexual exploitation of children in 2015.[19] Key recommendations from the report include establishing a comprehensive legal framework, enhancing international co-operation to investigate and prosecute OCSEA, the creation of a global permanent multi-stakeholder body, the empowerment of children and youth and greater corporate social responsibility. The Special Rapporteur continues to engage with state and non-state actors to implement these recommendations and the UN SDGs.

The 31st session of the UN Human Rights Council annual day on the rights of the child was dedicated to information and communication technologies and child sexual exploitation to strengthen knowledge and understanding among member states.

Council of Europe

The Ad hoc Committee for the Rights of the Child (CAHENF) was established to implement the Council of Europe's commitment to protect the rights of the child at inter-governmental level. The CAHENF oversees the implementation of the Council of Europe Strategy for the Rights of the Child (2016-2021),[20] which identifies the rights of the child in the digital environment as a priority area for action, leading to the adoption of the Committee of Ministers guidelines to respect, protect and fulfil the rights of the child in the

[18] https://violenceagainstchildren.un.org/sites/violenceagainstchildren.un.org/files/documents/publications/6._releasing_childrens_potential_and_minimizing_risks_icts_fa_low_res.pdf
[19] https://www.ohchr.org/Documents/Issues/Children/SR/A.HRC.28.56_en.pdf
[20] https://www.coe.int/en/web/children/children-s-strategy

digital environment, CM/rec (2018)7.[21] By implementing these guidelines, states can provide the framework within which children can fully exercise their rights in the digital environment, free from sexual exploitation or abuse.

The implementation of the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention) is monitored by the Committee of the Parties to the Convention (Lanzarote Committee). The Lanzarote Committee is composed of country representatives as well as representatives of civil society and international organisations and is also mandated to facilitate the collection, analysis and exchange of information, experience and good practices to improve capacity to prevent and combat sexual exploitation and sexual abuse of children. The second monitoring round of the Lanzarote Committee focuses specifically on the protection of children against sexual exploitation and sexual abuse facilitated by information and communication technologies.[22] The monitoring report is expected to be adopted in 2020 and will include practical recommendations to member states to strengthen the implementation of the Lanzarote Convention at national level. In addition, the Lanzarote Committee has adopted several documents to provide guidance on the ways in which the Lanzarote Convention applies to online grooming, to web addresses advertising CSAM, sexual offences facilitated by ICTs and to the exchange of sexually suggestive materials generated, shared and received by children.[23]

WePROTECT Global Alliance

The WePROTECT Global Alliance (WePROTECT) had its origins in two separate initiatives; the first was the "Global Alliance Against Child Sexual Abuse Online", launched in December 2012 by the European Commission and the US;[24] the second was the WePROTECT initiative established in 2014 by the UK.

By the summer of 2015 the two streams were merged, combining the Global Alliance's intergovernmental engagement with WePROTECT's broader coalition, which also included industry, law enforcement and civil society organisations. As of July 2019, membership stands at 89 governments, 25 civil society organisations and 20 technology companies, making WePROTECT the largest international initiative focused on online child sexual exploitation.

WePROTECT has developed a policy guidance tool in the form of a Model National Response,[25] which remains as a cornerstone document, along with a Global Threat Assessment, published in February 2018.[26]

Global Partnership to End Violence Against Children

The Global Partnership to End Violence Against Children is a multi-stakeholder initiative strongly linked with UNICEF and the World Health Organisation, taking as its principal focus programmes to deliver on the

[21] https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a
[22] https://www.coe.int/en/web/children/2nd-monitoring-round
[23] https://www.coe.int/en/web/children/lanzarote-committee#{"12441908":[2]}
[24] https://europa.eu/rapid/press-release_MEMO-12-944_en.htm
[25] https://www.weprotect.org/the-model-national-response
[26] https://www.weprotect.org

UN SDGs which run up to 2030.[27] SDGs 16 and 5 are the cornerstone of this work.[28] As its title suggests the Partnership's remit is wider than simply the online space but online is a key part of it. The majority of the resources in the Fund to End Violence Against children are committed to online child sexual exploitation. So far, the Partnership has raised US$68 million to support its work and has spent US$38 million with 48 different projects, of which $24m had been spent on projects to tackle online child sexual exploitation as of July 2018.

International Telecommunication Unit-UNESCO Broadband Commission for Sustainable Development

As with the Global Partnership, the Broadband Commission takes a strong steer from the SDGs. It is building on an annual process which exists within the International Telecommunication Union in which nations report on how they are developing broadband connectivity to advance social and economic goals. A sub-group of the Commission was established with the intention of encouraging Governments, telecommunications authorities and telecommunications industries to ensure that online child protection and children's rights were adequately reflected in their national plans.

With financial support from the World Childhood Foundation, the Oak Foundation and the Carlson Family Foundation, the Broadband Commission arranged for The Economist Intelligence Unit to publish the "Out of the Shadows Index", an index which "aims to shine a light" on child sexual abuse and exploitation across the world.[29] While the index covers a great many areas not directly or obviously linked to the internet, the internet nevertheless remains a major focus.

Institute for Human Rights and Business

The Institute for Human Rights and Business has produced an important publication which provides advice to companies on how to honour children's rights in the context of their online operations.[30]

The Child Dignity Alliance

The Child Dignity Alliance is closely associated with Pope Francis and the Pontifical Gregorian University in Rome. It focuses on research and religious outreach and engagement. It was launched in October 2017 and has since carried on its work through a series of working groups which look at a "prevention research programme", which is supported by US$20 million, and a Technical Working Group, which has produced a report on technologies available to combat OCSEA.[31]

[27] http://www.end-violence.org/fund
[28] https://www.undp.org/content/undp/en/home/sustainable-development-goals.html
[29] https://outoftheshadows.eiu.com/
[30] https://www.ihrb.org/uploads/reports/EC-Guide_ICT.pdf
[31] https://www.childdignity.com/founding

Mechanisms for collective action to strengthen specific legislative and policy frameworks to criminalise OCSEA, identify perpetrators and uphold the rights of the child-victim

The UN Committee for the Rights of the Child monitors the implementation of the UN Convention on the Rights of the Child (UNCRC) and of the Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography. Through this monitoring mechanism, states are encouraged to raise the level of protection procured to children by harmonising their legislation with these international standards.

The Lanzarote Convention and the Council of Europe Convention on Cybercrime (Budapest Convention) both mandate member states to make provision in national legislation to criminalise CSAM.

Chapter IX of the Lanzarote Convention provides that state Parties should co-operate with each other for the purposes of:

- preventing and combating sexual exploitation and sexual abuse of children (CSEA);
- protecting and providing assistance to victims; and
- investigations or proceedings concerning the offences established in the Convention.

The Lanzarote Convention also provides a legal basis for victims of offences that occur in the territory of a Party other than the one where they reside to make a complaint before the competent authorities of their state of residence. Furthermore, it provides a legal basis for mutual legal assistance in criminal matters or extradition in case of offences established under the provisions of the Lanzarote Convention in the absence of other such provisions, thereby filling any potential gaps in legislative frameworks.

International co-operation in the field of preventing and combatting CSEA may take the form of: training, research, analysis and monitoring, awareness raising among professionals and the general public, education and child participation. Whereas co-operation to protect and provide support to victims covers mechanisms to facilitate or strengthen: reporting, helplines and victim assistance, intervention programmes, recording and storing data in terms of sex offenders' registers and offender management.

By strengthening substantive and procedural legislative frameworks in line with international standards, states can better co-operate in the context of investigations and prosecutions to ensure: victim identification, perpetrator identification as well as: prioritisation of procedures and expedited procedures even where they originate from another jurisdiction.

In the context of OCSEA, the procedural safeguards contained in the Lanzarote Convention should be complemented by the provisions of the Budapest Convention, in particular as regards electronic evidence, mutual legal assistance and the 24/7 Network. In the context of OCSEA, such mechanisms are absolutely vital to ensure effective investigation and prosecution.

The EU Directive 2011/92/EU on combating the sexual abuse and sexual exploitation of children and child pornography sets down minimal standards for EU member states to prevent and combat this crime.[32]

Strategic Initiatives for policy development

There are a series of internationally based internet infrastructure bodies whose work directly impacts on questions affecting OCSEA. It is beyond the scope of this report to address these bodies in detail, however, for completeness, reference is made to two key ones: the Internet Corporation for Assigned Names and Numbers (ICANN),[33] and the Internet Engineering Task Force (IETF).[34] Both set technical standards which establish the baseline for how the internet works.

In the case of ICANN, national governments have a specific and exclusive responsibility for the operation of the Registry that operates their country code top level domain (.de, .fr, .sl etc.). These Registries can potentially act as exemplars of best practice which can leverage change in privately owned domains. Privately owned domains continue to constitute the great majority of all operational domains. In its latest annual report, the IWF identified three country code top level domains found to have significant volumes of CSAM. One of these is linked to a Council of Europe member (Russian Federation), the other two were not (Colombia and Tonga).[35]

In the case of the IETF, they "fast tracked" the development of a new technical standard, "Domaine Name System over https" (DoH),[36] which threatens to undermine or make wholly redundant long established measures for addressing OCSEA or protecting children from a wider range of legal but age inappropriate content.[37] At the time of writing, discussions are on-going with a range of industry players to ensure that where mandatory or voluntary child safeguarding measures are in place in a given jurisdiction, DoH providers should guarantee that these are not adversely impacted. This approach is relevant not just in relation to restricting access to CSAM or preserving other child safeguarding measures, but also for terrorist material, court mandated copyright infringing sites, and other Domain Name System (DNS) based sanctions.

ISPs or other online service providers can restrict access to CSAM by deploying a list of URLs known to contain it. The practice is now widespread. Such a list of proscribed addresses could be provided by a hotline or by law enforcement. If a user enters a web address or clicks on a link to a web address, in effect, the ISP or other online service provider checks to see if that address is on the proscribed list, in which case, access will be blocked. This is only possible because the DNS resolver can read the address.[38] The problem arises because DoH encrypts the address within the browser thereby making it invisible. The blocks are bypassed. This therefore threatens not only systems meant to limit access to CSAM but also other types of software that protect children, for instance family safety filters.

At one level DoH is already *fait accomplit.* DoH completed the IETF processes and is available for adoption. Individuals who are so minded can already use it. However, it is often far from simple to implement.

[32] https://ec.europa.eu/anti-trafficking/sites/antitrafficking/files/directive_2011_92_1.pdf
[33] https://www.icann.org/resources/pages/governance/aoc-en
[34] https://www.ietf.org/
[35] https://www.iwf.org.uk/report/2018-annual-report
[36] https://www.ietf.org/blog/doh-operational-and-privacy-issues/
[37] https://www.ispreview.co.uk/index.php/2019/04/big-uk-broadband-isps-have-big-concerns-about-dns-over-https.html
[38] https://www.computerhope.com/jargon/d/dns-resolver.htm

The worry would be if the standard was implemented by default within browsers.

The fact that private entities should have the power to make a decision of this nature unilaterally is cause for concern. The implementation of DoH may also result in the concentration of a large amount of data about web browsing and associated traffic in the hands of a small number of companies.

Mechanisms for collective action to strengthen governance structures and multi-stakeholder co-operation

International Center for Missing and Exploited Children (ICMEC)

ICMEC is a US based NGO that is a major actor in the field of online child safety.[39] Apart from publishing the legislative review referred to above, its portfolio of activities has recently expanded considerably to include analysis of country practices and the provision of training, particularly with law enforcement.[40]

Since 2006, ICMEC has been monitoring the legal framework addressing CSAM in all UN member states. Their latest report (2018) shows that the Budapest and Lanzarote provisions have been unevenly acted upon by Council of Europe member states.[41]

ICMEC monitors and reports on countries' performance under five specific headings:

- Is there legislation specific to CSAM?
- Is CSAM defined?
- Does the law recognise the existence of technology facilitated crimes?
- Is "simple possession" of CSAM illegal?
- Is there mandatory reporting of CSAM by ISPs to the police?

An overview of how different countries fulfil these criteria is available in the annual ICMEC report.[42] Compliance with requirements for mandatory reporting of CSAM by ISPs to the police is not generally regarded as being an essential indicator of best practice. However, compliance with each of the other four criteria is widely recognised as constituting a minimum acceptable standard. It will be noted that most, but not all, Council of Europe member states meet the minimum of four out of the five standards and a small number meet five out of five. For an overview of member state performance please see the baseline mapping of member state responses to prevent and combat online child sexual exploitation and abuse.

[39] https://www.icmec.org
[40] https://www.icmec.org/wp-content/uploads/2017/06/GlobalTrainingCatalog201718_WithFinalEdits-1.pdf
[41] ICMEC (2018) Child Sexual Abuse Material: Model legislation & Global Review, The Koons Family Institute on International Law & Policy, USA, available at: https://www.icmec.org/wp-content/uploads/2018/12/CSAM-Model-Law-9th-Ed-FINAL-12-3-18.pdf
[42] https://www.icmec.org/wp-content/uploads/2018/12/CSAM-Model-Law-9th-Ed-FINAL-12-3-18.pdf

Global Kids Online

What started initially as a UK-specific research project (UK Kids Go Online) led by Professor Sonia Livingstone, with EU help, evolved to become EU-Kids Online now led from the Hans-Bredow Institute in Hamburg and in turn, with the engagement of UNICEF, into "Global Kids Online". This initiative has fourteen participating countries, including several Council of Europe member states.[43]

Global Kids Online is one of a comparatively small number of truly transnational initiatives in the field where common standards and approaches have been agreed and are being actively deployed. In part this has been possible due to the long-standing tradition of international collaboration at operational level in the academic world in such a way that data can be collected and compared on an international level.

The kind of data collected by Global Kids Online is extremely valuable and important both in its own right but more particularly to enable international benchmarks and comparisons to emerge. High level data of the kind provided are an important starting point which can help provide a focus for research in more specific or narrowly defined areas of interest, for instance approaches to training different professional groups or helping parents help their children. The larger the dataset, the more reliable and therefore the more valuable the data are which is why it is important for as many countries as possible to engage with Global Kids Online. If it is ever going to be possible to develop sound mechanisms for evaluating different approaches to addressing the online child safety and online child rights, agenda baseline data of the kind being collected and analysed by Global Kids Online is likely to be essential.

Better Internet for Kids

The flagship EU initiative in the field of children's rights online and online child protection is the Better Internet for Kids.[44] Historically it has been the largest single source of funding for programmes and research in this field, although in recent years the level of resources devoted to its programmes has diminished. The EU is responsible for the now global "Safer Internet Day" (SID) which appears to have reached into and been taken up by most countries in the world. The next SID is Tuesday, 11th February 2020.

The Council of Ministers and other EU institutions, particularly the European Parliament, have been important mechanisms for developing political engagement at the highest levels within member states. The regular conferences have also played an important part in developing higher levels of understanding and engagement with the issues and in sustaining or developing a transnational network of civil society organisations that specialise in children's concerns in the online environment. Without the financial and organisational support the EU was able to provide, it is very unlikely this would have happened or else it would have happened at a much slower and less certain space.

[43] http://globalkidsonline.net/
[44] https://www.betterinternetforkids.eu/

The Family Online Safety Institute

The Family Online Safety Institute (FOSI) had its origins in the USA and has a global focus.[45] Its major output is an annual event in Washington that gives member companies an opportunity to showcase their work in the online child safety space and to engage with researchers.

The FOSI Global Resource and Information Directory (FOSI GRID) was an extremely welcome initiative that was first launched in 2010. This was the first time any organisation appeared to have recognised the importance and value of developing an informational database across a broad range of headings connected with the position of children as internet users.

FOSI GRID promised to provide a single platform to access to raw data translated into English and to standardised data drawn from original sources about the position of children as internet users and measures taken to protect them or enhance their rights. It was hoped and envisaged that the FOSI GRID would eventually become an openly available resource for use by researchers, campaigners, policy makers, Governments, child protection and child rights specialists, journalists and anyone else with a relevant interest. It was intended that interested parties would be able to see what the position was in their own country but also to compare it with neighbouring or other territories, to spur improvements within individual countries but also to act as a way of monitoring the behaviour of individual companies across jurisdictions. If company x was willing to protect children in jurisdiction y, why would it not be willing to do the same or something similar in jurisdiction?

Initial financial support for the FOSI GRID came from UNICEF and Microsoft but when these funds were not renewed, updates to the GRID were suspended.

The GRID is still visible online but because it is getting more and more out of date and becoming less and less valuable. It could potentially become a liability because the information on the site may now be wrong in light of changes that have taken place in different countries.

This was a hugely ambitious project and the costs associated with its development were substantial. If it is to be revived it seems likely that a more secure and sustainable funding and organisational base will be essential. This is discussed further below in the context of a proposal to establish a Global Observatory.

[45] https://www.fosi.org/

Mechanisms to strengthen law enforcement capacities to investigate cases of OCSEA, including the existence of dedicated law enforcement units

Law enforcement agencies and children's workforces operate within the confines, regulations, standards and cultural expectations of the jurisdictions within which they are based. To that extent, the scope for developing internationally recognised training packages or regimes must be limited. There nevertheless remains a great thirst for knowledge about the approaches, costs and outcomes that have been tried in different countries. There is a widespread sense that people can learn a huge amount from each other and that such learning can help them adapt apparently successful models to their local setting. *Ad hoc* presentations on different initiatives are quite common at international events. What has been lacking, hitherto, has been any kind of systematic attempt to draw the information together and make it available to practitioners to maximise its utility.

There are a variety of transnational organisations which offer help with training in the field of online child protection and related subjects. Several also have regional offshoots but it is true to say that, in the field of training, there are, as yet, no globally recognised or established standards. This is true in many fields consequently, if there is a need for practitioner training or support, in effect one is forced to choose based on the reputation or standing of the organisation offering to provide it.

The Crimes Against Children Conference is held every year in Dallas, Texas. It has evolved over the 30 years to become not just an important focal point for training law enforcement officials from the USA but for law enforcement officers and professionals from all parts of the world who are concerned with all types of crimes against children. There is a major focus on online crimes against children. In 2018, there were more than 5000 participants.

International Child Exploitation database

The core policing institution for all Council of Europe member states will be International Criminal Police Organization (INTERPOL) and for EU member states EUROPOL also plays an extremely important role. INTERPOL and EUROPOL both organise a range of conferences and training opportunities to help develop the capacity of national police forces to tackle OCSEA.

INTERPOL hosts the globally important International Child Exploitation database (ICSE).[46] In the joint INTERPOL and ECPAT International report it was announced that ICSE would be upgraded and modernised to improve its functionality and increase its utility not only as an investigative tool but also as a source of

[46] https://www.interpol.int/en/How-we-work/Databases/International-Child-Sexual-Exploitation-database

intelligence about child sex abuse.[47]

ICSE holds some 1.5 million images and has been instrumental in helping to identify over 19400 victims and 8900 offenders. However, as of May 2019 only 60 countries, out of a possible 194, plus EUROPOL participate, although data from over 80 countries had been uploaded.[48]

To be able to subscribe to ICSE, the relevant law enforcement agency in the country concerned has to have developed its work in the field to a certain standard and be able to meet specified technical, security and training protocols. The fact that fewer than one third of countries eligible to join have in fact joined on the face of it is troubling.

It has to be a key ambition to ensure every police force in the world has the ability to upload data to and be able to interrogate ICSE. Meanwhile other countries' police forces, including several Council of Europe member states are developing their own databases but it is understood there is a widely shared ambition to ensure that all of these databases can interact and that therefore there will eventually be, in effect, a single point of entry.

The advantages of having a single global database of images, or at any rate of having a single point of access to a network containing all known CSAM, are likely to be considerable to optimise the use of investigative time and resources.

Virtual Global Taskforce

The Virtual Global Taskforce (VGT) co-ordinates a range of activities connected with online child protection.[49] Three Council of Europe member states are part of the VGT: the Netherlands, Switzerland and the UK. The "FiveEyes" co-operation between intelligence services have also been working closer together across a broad range of cybercrimes including crimes against children.

[47] https://www.ecpat.org/wp-content/uploads/2018/02/TOWARDS-A-GLOBAL-INDICATOR-ON-UNIDENTIFIED-VICTIMS-IN-CHILD-SEXUAL-EXPLOITATION-MATERIAL-Summary-Report.pdf
[48] https://www.interpol.int/en/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database
[49] https://virtualglobaltaskforce.com/vgt-strategic-goals /

Mechanisms for collective action to strengthen offender management

Prevention and Probation

International Society For The Prevention Of Child Abuse & Neglect (ISPCAN) is a global body with the largest reach.[50] It has links to organisations that work at a regional and national levels such as the Association of Child Protection Professionals (formerly BAPSCAN)[51] and NOTA, a body that originally worked largely with Probation Officers working with aggressive sex offenders but which has since evolved to become an organisation that supports a range of professionals engaged in preventing all forms of sexual abuse.[52] The Association For The Treatment Of Sexual Abusers (ATSA), also provides key resources.[53]

Practice Example: Dunkerfeld

The Dunkerfeld Project is based in Berlin where it is linked to the Charité Hospital. There is a limited amount of information about it in English but Dunkerfeld is widely regarded as a world leader in providing clinical and support services to individuals who are sexually attracted to children (paedophiles and hebephiles) and want help controlling their sexual urges, but are otherwise unknown to the legal authorities. The term "Dunkelfeld" is German for "dark field". The project began in June 2005 with a large media campaign to contact paedophiles and hebephiles who wanted help from clinicians to manage their paraphilia. The campaign pledged medically confidential treatment, free-of-charge. It was initially funded by the Volkswagen Foundation, and has been financially supported by the German government since 2008. The project's slogan is "You are not guilty because of your sexual desire, but you are responsible for your sexual behaviour. There is help! Don't become an offender!"

Between 2005 and 2018, 10500 participants had contacted the network "Don't Offend" and 1,783 had been offered therapy. The therapy offered has three main components. Patients are encouraged to accept their sexual inclinations and involve relatives or partners in the therapeutic process. Cognitive behaviour therapy is used to improve coping skills, stress management, and sexual attitudes. Drugs that reduce general sex drive, such as serotonin reuptake inhibitors and anti-androgens, may also be offered.[54]

There are projects similar to Dunkerfeld in the UK and the USA. These are called "Stop It Now".[55]

[50] https://www.ispcan.org/who-we-are/
[51] https://www.childprotectionprofessionals.org.uk/
[52] https://www.nota.co.uk/
[53] http://www.atsa.com/
[54] https://www.dont-offend.org/story/10-500-people-asked-for-help.html
[55] https://www.stopitnow.org.uk/lucy-faithfull-foundation.htm

Mechanisms to strengthen provision of end-to-end support to child-victims of OCSEA

Reporting Hotlines

As previously discussed in this paper, INHOPE was created as a global association to allow the rapidly developing network of national hotlines to exchange information and forge working links with INTERPOL. INTERPOL was concerned not only with assisting in the removal of images or restricting access to them, it took on a key role in victim identification. Victims and perpetrators could be anywhere in the world. Consequently, an agency capable of, and accustomed to working across national boundaries, was essential.

The operation of hotlines

As a major feature of the OCSEA landscape, hotlines require a more detailed examination.

There is a recurring tension between those who think only law enforcement or another state agency should deal with CSAM, and those who see the value of hotlines being NGOs that co-operate closely with law enforcement but operate at arms-length, if in varying degrees.

In most countries in the early days, hotlines emerged as NGOs. Increasingly, law enforcement agencies are improving their ability to engage with work of this kind. However, it remains the case that, at least insofar as reporting CSAM is concerned, members of the public are much less likely to be willing to deal directly with the police as compared to a non-police body.

As of January 2019, INHOPE had member hotlines in 41 countries. The EU Directive 2011/92/EU on combating the sexual abuse and sexual exploitation of children and child pornography recalls that the establishment of help-lines or hotlines should be considered and promoted,[56] every EU member state currently has at least one hotline. Most countries only have one hotline although a small number, for instance Germany and Italy, have more than one. The EU contributes to the funding of at least one hotline in every EU member state although in some instances the contribution can be as low as 10% of total operating costs.

The balance of the funding required to sustain a hotline can come from a wide range of sources, including the national government. Often, there will be some contributions from high tech businesses. However, there is no single consistent funding model which raises concerns about their longer-term sustainability.

[56] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32011L0093

Moreover, while INHOPE sets minimum operational and other standards, for example every hotline must have the support of the national government and law enforcement, there is no single governance model. A wide variety of arrangements exist, reflecting local conditions and, usually, the history of how the hotline came to be established in the first place.

Article 12 of the Lanzarote Convention obliges state parties to take the necessary legislative or other measures to encourage reporting, without imposing a specific mechanism. However, in the Committee of Ministers Recommendation CM(2018)7 on Guidelines to respect, protect and fulfil the rights of the child in the digital environment, the establishment of reporting mechanisms for CSAM is strongly endorsed and recommended as a starting point for actions to combat CSAM and as a public acknowledgement that actions are being taken.

The Council of Europe Baseline Mapping of member state responses to prevent and combat online child sexual exploitation and abuse, provides an overview member states with operational hotlines. It will be noted that there are several Council of Europe member states where there appears to be no know reporting mechanisms inside or outside of the INHOPE framework.

Helplines

Article 13 of the Lanzarote Convention requires state parties to encourage and support mechanisms such as helplines, and in practice many hotlines also act as children's helplines. Within the EU, every hotline which is funded by the Commission is part of the national Safer Internet Centre which helps connect it with a broader range of concerns for children's wellbeing. The Insafe network of Safer Internet Centres (SICs), include helplines which provide information, advice and assistance to children, young people and parents on how to deal with harmful content, harmful contact (such as grooming) and harmful conduct such as (cyberbullying or sexting).[57]

[57] https://www.betterinternetforkids.eu/web/portal/policy/insafe-inhope

Mechanisms to strengthen education and awareness raising initiatives to prevent OCSEA in member states

ICT Coalition

The ICT Coalition is a voluntary association of 20 tech companies that have relationships of one kind or another with the EU.[58] It acts as a mechanism for companies to make public commitments about what they are doing to advance online child safety, and the Coalition funds an independent researcher to determine whether or to what extent the companies are keeping the promises they made. The first reports were published in 2014 and some additional ones appeared in 2017 and 2019.

Checks and balances on industry: Data Privacy Commissioners

The emergence of children as a major constituency of internet users has meant that the privacy authorities and privacy lawyers are increasingly involved with issues connected with children's rights in the online environment. Within the EU, the General Data Protection Regulation made important stipulations concerning the minimum age at which children could be considered competent to decide for themselves whether or not to join a service, namely without the service having to seek verifiable parental consent. Without any consultation with experts and at the very last minute, the EU decided to allow a multiplicity of age limits (between 13 and 16). No one is yet clear what the implications are of having, on the same platforms operating simultaneously in different jurisdictions, young people and possibly their parents who have been verified according to different standards. Equally, there is uncertainty about the implications for children of the new rules about "profiling", that is collecting data about children's activities in order to target advertisements at them. In addition, it seems some companies have decided to abandon the need to obtain consent by increasing their use of "legitimate interest" as the basis of collecting and processing data of persons under the age of 18.

Industry specific codes of practice are to be devised and there are anxieties that the data protection authorities in many jurisdictions are not sufficiently familiar with the position of children as internet users so as to engender confidence in the outcome of the processes that will be used to create the codes.

These developments all point in the same direction. Child protection professionals and policy makers need to become more engaged with the world of privacy lawyers and privacy institutions, and vice versa. At the moment the resources of both are severely stretched.

[58] http://www.ictcoalition.eu/

Data Privacy Commissioners meet on an international basis but it is not clear whether or to what extent they welcome or permit interests from the "non-privacy world" to engage.

The European Data Protection authorities meet annually, the last meeting being in Albania in May 2019. There is also a global meeting, to be held again in Tirana, in October 2019.

Conclusions

A global or regional observatory, the need for a Think Tank

In many parts of the world there is an enormous amount of activity taking place on or around children's online rights and children's welfare online. There is a great thirst for knowledge about these issues, particularly in countries where fast broadband speeds and WiFi connectivity are starting to become available for the first time to the mass of the population and to the mass of children.

Resources and information developed within different countries showing examples of good practice or discussing how parents, teachers and others have tried to face the challenges of children becoming major users of the internet, has tended to remain in that country. This is particularly the case if it has been written in a language other than English or one of the other major world languages.

There is currently no on-going, reliable or predictable mechanism for collecting such information or resources, for assessing its quality and therefore its likely usefulness to people outside the countries where it was created. This in turn has been a major factor impeding the development of internationally recognised standards, enabling international comparisons which has impeded any substantial degree of harmonisation of practice. It has also made it easier for companies to apply different policies and standards in different jurisdictions. For example, Starbucks restricts access via WiFi in half a dozen or so countries but not in every country where it operates. Why is that? Don't children everywhere deserve the same sorts of protection? If children's organisations and governments everywhere knew that Starbucks had done this for other people's children, is it not likely they would want them to do it for theirs or explain why not?

Ad hoc presentations at different international events, occasional seminars, and the like, certainly have their place in reaching out to leadership groups. But that is not the same as having an established, systematic, on-going mechanism which not only performs the gathering-in function, but also has a brief to translate, prepare and present the materials in ways which are timely, targeted and which maximises their usability.

This situation deprives governments, policy makers, the research community, civil society and the children's workforce, of access to the widest range of resources to help them in their work. It underlines the asymmetry that exists as between these public, non-commercial actors and powerful, rich corporate interests, who will always have the ability to track changes and keep up to date in terms of technical changes and policy developments that could impact their markets.

In an age of information overload, simply asking people to join another email chain, list-server or to sign up for a Newsletter is not sufficient. For maximum impact, the resources need to connect with people on the ground who can make use of them, and that means the publishers have an outreach responsibility to identify key people and help develop an international network. This would bring yet more benefits as it would mean civil society and governments would be better placed to take part in important international arenas such as the Annual Internet Governance Forum and to participate in other multi-stakeholder forums such as ICANN and the IETF.

In conclusion, a feasibility study should be commissioned to determine the operational parameters and likely costs of establishing a global observatory or think tank, with a brief to become the world's foremost resource for policy makers and civil society organisations, with an interest in children's rights and children's well-being in the digital environment. This would involve close consultation with existing major policy institutes and children's organisations. But it would also recognise the need to develop a centre of expertise in the technology space which will require a special focus and which does not currently exist to any substantial degree.

Regardless of how or why an image, video or stream depicting the abuse of a child is present online, it is of the utmost importance to remember that behind each image, video or stream there is a real child, suffering, who should be treated and supported as a victim. As the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention) recalls: a wide range of stakeholders are in charge of protection from, prevention of and the fight against sexual exploitation and abuse of children, including in the online environment.

The very nature of this crime requires these stakeholders to co-operate beyond regional and national borders to identify and rescue victims, locate and apprehend perpetrators and remove child abuse material to prevent re-victimisation. This comparative review provides an overview of the mechanisms available at international and pan-European level to prevent and combat online child sexual abuse and exploitation and makes the case for further engagement with these mechanisms.

ENG

www.coe.int/children

The Council of Europe is the continent's leading human rights organisation. It comprises 47 member states, 28 of which are members of the European Union. All Council of Europe member states have signed up to the European Convention on Human Rights, a treaty designed to protect human rights, democracy and the rule of law. The European Court of Human Rights oversees the implementation of the Convention in the member states.

End Violence Against Children
THE FUND

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE