Child Dignity
in the Digital World

Child Dignity Alliance

Technical Working Group Report

Contents

Foreword by Child Dignity Alliance Technical Working Group

In 2017, the Centre for Child Protection at the Pontifical Gregorian University in Rome hosted the World Congress on Child Dignity in the Digital World, in partnership with the WePROTECT Global Alliance and Il Telefono Azzurro. Dozens of the world's online safety leaders joined the Congress to discuss the international fight against online child sexual exploitation.

A 'Declaration of Rome' was presented, and accepted, by Pope Francis at the World Congress. In order to implement the commitments made in the Declaration, the Child Dignity Alliance convened six working groups so as to stimulate global awareness of the global CSAM pandemic through research, policy and interfaith collaboration.

The working groups were involved in the following work:

- Prevention research, chaired by Fr Hans Zollner
- Foundational research on harm to children in the digital world, chaired by Prof Ernesto Caffo
- Building global awareness, chaired by Baroness Joanna Shields
- Building a multi-faith coalition to protect children in the digital world, chaired by Ernie Allen, and
- Protecting children from internet pornography, also chaired by Ernie Allen.
- Technology and its impacts on children, chaired by Julie Inman Grant

The Technical Working Group was charged with examining the role of technology in combatting the proliferation of online child sexual exploitation and abuse imagery. The working group is comprised of some of the world's leading experts in this area, including Julie Inman Grant; Baroness Joanna Shields OBE; Baroness Beeban Kidron OBE; Jacqueline F. Beauchere; John Carr OBE; Peter MacKay QC; Christian Berg; Brooke Istook; and John Stix.

A focus of this report is on the need to dismantle the chief technical, legal and policy silos that are frustrating real collaboration among law enforcement, industry, government and the non-government sector. As a global community, we need to embrace innovation, safety and agility as core tenets of technology design.

The report also highlights the need to acknowledge that some of the impediments to collaboration are more perceived than real, more the result of custom and practice than unsolvable. More often than not, these are based on risk avoidance, lack of trust in systems, procedures and intent, and an inconsistent application of law and policy. In some cases, barriers are a legacy of organisational history, and no longer reflect the issues that are most relevant today.

There is an urgency to this mission. We must strive to take every step we can, individually and as a global community, to combat the scourge of online child sexual exploitation and abuse wherever it is found. This report highlights that this can be achieved. Despite the barriers that have been identified, there is real hope. Advancements in technology, machine-learning and artificial intelligence have the potential to radically transform the landscape. As a global community, we need to do all that we can to ensure that we harness the possibilities that they offer in a unified and integrated way.

The Technical Working Group commends this report to leaders around the world who are now poised to take our work forward.

Executive summary

This report surfaces what the Technical Working Group identified as the chief barriers to an optimal global response to online child sexual abuse material (CSAM) within three sectors: law enforcement, industry and government. The barriers identified are explained in detail in the report, and specific recommendations made for each sector. Recommendations are also provided for joint action.

Two overarching themes have also emerged. First, the need for greater standardisation of process, practice and policies; second, the need for greater collaboration, coordination and inter-operability across stakeholders and functions, nations and jurisdictions.

Barriers to optimal global response

As noted in the report, one of the major issues facing law enforcement and hotlines in this crime type is the sheer volume of images and videos requiring initial analysis and investigation. Classifying CSAM at scale remains a serious constraint for police. There are a number of classification schemata in use across jurisdictions and no single universal framework for the categorisation of images and videos. When police are working with datasets from multiple sources, the lack of a unified approach to categorising images slows down the work of victim identification, needlessly exposes analysts to material already classified, and increases the risk that crucial victim identification clues will be missed.

Through the course of preparing this report, it became clear that partnerships between law enforcement and the technology industry are essential if police are to maintain an edge against those producing and sharing CSAM. However, a barrier exists: law enforcement agencies (LEA) are not well-suited to the processes of technology design and implementation, or long-term product support.

Any products developed in this domain must reflect the nature of the threat landscape. Given the size of data-sets relevant to investigating online CSAM, tools must work at scale to ingest and analyse 'big data', requiring automated and intelligent workflows. For industry to develop such tools, they need access to relevant annotated datasets, through which machine intelligence algorithms can be trained.

Yet, police forces are reluctant to share this data, due to concerns about security and confidentiality. These concerns are entirely valid, as it may be possible for bad actors to gain an advantage if they were given access to a database of digital CSAM fingerprints. But a compromise should be pursued. If even well-vetted members of industry are denied training data, innovation will be hampered, dulling the edge that would otherwise be provided to LEA through advanced technology capabilities.

For industry, it is important to recognise that their role is not limited to simply developing tools. As the owners of networks and platforms that form the backbone of the internet, companies should be expected—and possibly mandated by government—to ensure they take proactive steps to combat CSAM. This should include deploying hashing algorithms so that child abuse imagery traversing or stored on their networks is detected. This measure ought to be only one component of a comprehensive approach to monitoring traffic for indicators of exploitation and abuse. Where appropriate, other tools should be used, for example webcrawlers and text analysis.

This paper evidences the relatively sparse take-up of these technologies by companies domiciled in the UK and United States. Recent announcements made by some of the big tech firms show that industry has the potential to make considerable advances. However, there is far more that industry as a whole can, and should, be doing to harden their infrastructure against its misuse by predators who make it their business to abuse and exploit children.

A final barrier exists to creating an optimal response to CSAM: while a degree of harmonisation between nations is desirable, many countries have failed to sign or ratify existing treaties, protocols or other convention-like instruments. Alarmingly, there are 35 countries that have no legislation criminalising child sexual abuse imagery. Three-quarters of states that have enacted statutes at the domestic level do not define CSAM, making prosecutions for possession and distribution difficult, if not impossible. The result is a large zone of impunity for those intent on producing, distributing and monetising CSAM.

Even when states have fully implemented criminal and regulatory instruments to control CSAM, the efforts of police and prosecuting authorities can be hampered by inconsistent terminology and definitions. Cooperation can be fragmented when jurisdictions disagree about what constitutes online child exploitation, or which thresholds are relevant to a prosecution. Taken together with the general failure of legislation to keep pace with and reflect changes in the use of technology, mismatched standards can work to frustrate effective and timely responses by law enforcement.

Based on recommendations in this report we hope to assist in breaking down silos, tackling fragmented approaches and addressing the current restrictive policies and procedures—leading to positive developments and outcomes.

BARONESS KIDRON

Baroness Beeban Kidron is the Founder and Chair of 5Rights Foundation. She is a Crossbench member of the House of Lords, where she sits on the Communications Committee. She is a Commissioner on the UN Broadband Commission for Sustainable Development and a member of; The Royal Foundation Taskforce for the Prevention of Cyberbullying; WeProtect Child Dignity Alliance Technical Working Group; The Global Council on Extended Intelligence; Arts Council England's Commission on Creativity and Education; and President of Voluntary Arts. Kidron has worked for 35 years as an award-winning film director and co-founded the educational charity, Into Film.

CHRISTIAN BERG

Christian Berg has founded the Safer Society Group which consists of the three companies NetClean, Griffeye and Paliscope, all with a focus to create a safer society. NetClean has a suite of products to stop child sexual abuse content, Griffeye has the world's premier solution to investigate cases involving huge volumes of images and videos and Paliscope is the tool for online investigations. Mr. Berg has two Master's Degrees; Automation Engineering from Chalmers University of Technologies and Innovation and Entrepreneurship from Chalmers School of Entrepreneurship.

BARONESS SHIELDS

Rt. Hon. Baroness Joanna Shields OBE, a technology industry veteran and parliamentarian, is currently Group CEO of BenevolentAI. She has previously served as the United Kingdom's Minister for Internet Safety and Security and Parliamentary Under Secretary of State from 2015 to 2017, and the Prime Minister's Special Representative on Internet Safety. She is a Life Peer in the House of Lords. Baroness Shields career began in Silicon Valley and spans over 25 years, during which she held key executive roles at leading technology companies: EFI, RealNetworks, Google, Aol and Facebook. A committed advocate of child safety online, she founded the WePROTECT Global Alliance, which seeks to eradicate child sexual exploitation globally.

BROOKE ISTOOK

Brooke oversees all of Thorn's programs, products and operations to ensure effective and efficient execution of Thorn's mission. Brooke led the development and deployment of Spotlight, Thorn's sex trafficking investigation tool with over 7,000 law enforcement users, and manages Thorn's international partner relationships. Prior to joining Thorn, Brooke spent over 12 years working in IT consulting, operations, and program management, supporting Fortune 500 clients in telecommunications and entertainment. Ms Istook holds B.S. in Business Administration from the University of Alabama and an M.A. in Cross-Cultural Studies from Fuller Seminary.

JACQUELINE BEAUCHERE

Jacqueline Beauchere is the Chief Online Safety Officer at Microsoft. In this role, Ms. Beauchere is responsible for all aspects of Microsoft's online safety strategy, including internal policy formulation, influence over consumer technology features, and external engagement. She serves on the international advisory board of the WePROTECT Global Alliance; is a member of INHOPE's Advisory Board, as well as the European Commission's new Better Internet for Kids Advisory Board. Prior to Microsoft, Ms. Beauchere was an attorney in private practice. A second-career lawyer, she spent 12 years as a journalist and editor, most recently with Reuters America.

JOHN CARR OBE

John Carr OBE is one of the world's foremost authorities on children's and young people's use of the internet and associated new technologies, and is or has been a Senior Expert Advisor to various UN and EU online safety and security bodies. He is also an Expert Advisor to Bangkok-based global NGO ECPAT International, and to the European NGO Alliance for Child Safety Online (eNACSO), and Secretary of the UK's Children's Charities' Coalition on Internet Safety (CHIS). Mr Carr is a Senior Visiting Fellow at the London School of Economics and Political Science.

JOHN STIX

As co-founder of one of Canada's largest telecom and internet companies Fibernetics, John has lead an international team by example and empowerment. He witnessed the positive change that occurred within his own company when he decided to focus on unity, teamwork, empathy, happiness and gratitude. After introducing his "I'M IN" corporate initiative, John received the Best Employer Branding award in 2015 from the Canadian Human Resources. As an entrepreneur, John has been a visionary, thought leader and mentor taking start-ups to enterprise-level organizations and figuring out innovative ways to keep all employees highly engaged, through all stages of growth and transformation. John's latest venture as president of KidsWifi, is allowing him to transform the way parents view the internet and to protect kids globally while online.

JULIE INMAN GRANT

Julie Inman Grant is a globally-recognised online safety expert with more than 20 years' experience in the technology industry. She has performed senior roles with Microsoft as Global Director, Privacy and Internet Safety; Twitter, as Director of Public Policy, Australia and South-East Asia; and Adobe, as Director of Government Relations APAC. She is currently the Australian eSafety Commissioner at the Office of the eSafety Commissioner.

PETER MACKAY

Peter MacKay is a Partner in the Baker McKenzie Toronto office. Prior to joining the Firm in 2016, Peter MacKay, PC, QC (Privy Council and Queen's Counsel), served in the Parliament of Canada for over 18 years and in a ministerial post in the Canadian government for almost ten years after the Conservative Party formed a government in 2006. Most recently, he served as Canada's Attorney General and Minister of Justice until November 2015, a position to which he was appointed in 2013. Prior to this post, Mr. MacKay served as the Minister of National Defence for six years and held joint cabinet positions as Minister of Foreign Affairs and Minister for the Atlantic Canada Opportunities Agency for 18 months.

Recommendations

Government initiatives

1. Governments should adopt the recommendations in this report and require industry to develop procedures that ensure CSAM on their networks is detected, reported and speedily removed. This will require legislative and policy clarity about industry's obligations, penalties for non-compliance, and the development of guidance, information and resources to aid and assist industry to comply.
2. Governments, through the Child Dignity Alliance and the WePROTECT Global Alliance, should immediately commence work on ensuring that their domestic legislative frameworks comply with the International Centre for Missing and Exploited Children's Model Legislation; and that consistent definitions and terminology are adopted alongside these efforts that are consistent with the 'Luxembourg Guidelines'.
3. Technical data of any kind, including hash data sets, relating to child sexual exploitation and abuse imagery should be defined and treated as 'global assets'. Hashes should be made available across trusted sectors and jurisdictions to:
    - aid law enforcement case management efforts (especially victim identification)
    - assist with industry efforts to innovate and develop new identification/classification technologies.
4. Governments should, to the greatest extent possible, and being respectful of legitimate privacy rights, remove any doubt or ambiguity about the legality of internet businesses deploying technical tools in the fight against CSAM.

Law enforcement initiatives

5. Leading governments, including the governments of the United States, the United Kingdom, Australia, Canada and New Zealand should support INTERPOL's planned upgrade of the ICSE database so as to:
    - produce greater consistency of practice in relation to the annotation of hashes and data entry
    - guarantee greater consistency and maintenance of data concerning identified and unidentified victims
    - encourage greater take up of high-quality remote connections
    - consider additional metrics that might help identify a greater number of victims.
6. There should be efforts made at the supra-national level, through appropriate multilateral working groups, to implement a single standard framework for the classification of child abuse imagery. This should be adopted by, at a minimum, the 'Five Eyes' countries of Australia, the United Kingdom, Canada, New Zealand and the United States. In addition, those nations should contribute to and support development of tools allowing for the 'translation' of categories from one jurisdiction to another.

Industry initiatives

7. Major technology companies like Facebook, Twitter, Google, Snap, Microsoft and others should continue to support the efforts of law enforcement, government entities and not-for-profit hotlines, including through sharing enhanced key technical and operational data, for example hash data.
8. Industry must work collectively to reduce the siloed and fragmented patchwork approach to the development of technical tools such as AI classifiers and hashing algorithms. It must be a guiding principle that technology which tackles child sexual abuse imagery is shared, standardised and placed at the disposal of all parties involved in fighting against this crime, regardless of sector.
9. The technology industry should work collaboratively and exchange operational data and intelligence about those abusing their networks to share and distribute child sexual abuse imagery. Part of this might include larger companies providing more formalised and systematic support against child sexual abuse imagery to smaller industry members as part of an 'industry leadership' role.
10. Internet governance bodies, including ICANN and registry operators such as Verisign, must take robust and transparent steps to improve the verification of customer identity when new domains are registered or renewed. They must also ensure that those representing and advocating for children's rights are fairly and robustly represented in their fora.
11. To ensure that predators are not exploiting online services to groom and abuse children, owners of interactive platforms and services should make better use of the data they collect about their users. This will enable them to proactively identify threat actors and vulnerable users—especially children—and ensure measures are in place to allow swift and effective intervention, disruption and support.

Joint initiatives

12. To expedite investigations and accelerate innovation industry must develop robust and universal cooperation frameworks and standards for legal interoperability for data and intelligence sharing between law enforcement agencies globally, as well as between law enforcement and trusted private entities.

13. Industry should be strongly encouraged, or even required through domestic legislation, to:

    - adopt PhotoDNA and PhotoDNA for Video or other child sexual exploitation and abuse material identification and sharing technologies
    - be required to scan their networks, platforms and services, or take similar active measures, as a default operating procedure, to detect known child sexual abuse imagery content, including so-called 'passthrough' services
    - enforce standards and codes of conduct against illegal behaviour on their platforms
    - implement Safety by Design frameworks, codes of practice or minimum standards.

14. Global frameworks that are established to advance these recommendations should embody child sexual abuse imagery efforts and human rights obligations, while balancing the need to maintain standards of privacy, security and safety.

15. Governments, governance groups and industry should support the Child Dignity Alliance and the WePROTECT Global Alliance to maintain and improve a technical inventory (a central repository of current information about tools and technologies) to assist law enforcement to investigate, identify victims and manage CSAM cases.

Overview of the Technical Working Group

The Child Dignity Alliance Technical Working Group (TWG) was formed in April 2018. It was convened alongside five other working groups to drive forward aspects of the 'Declaration of Rome'—presented to Pope Francis on 6 October 2017 following the World Congress: Child Dignity in the Digital World. The Declaration of Rome concluded that:

'In this era of the Internet the world faces unprecedented challenges if it is to preserve the rights and dignity of children and protect them from abuse and exploitation. These challenges require new thinking and approaches, heightened global awareness and inspired leadership'

The focus of the Technical Working Group was to harness and promote innovation, investment and commitment among the global digital community to address and combat the proliferation of online child sexual exploitation and abuse imagery.

The TWG is chaired by the eSafety Commissioner of Australia, and includes eight full-time members,[1] representing industry, the legal profession, non-Government organisations, an independent child safety consultant, a Member of UK House of Lords, and a founder of the WePROTECT Global Alliance.

The focus of this report is to shine a light on some of the intertwined technical, legal and political barriers that currently impede the global community in more effectively and seamlessly combatting online child sexual abuse. It also proposes solutions that the Technical Working Group believes would go some way toward breaking down these barriers. The report is divided into three sections, highlighting the specific barriers relating to law enforcement, industry and the legal and policy system.

Overview of online CSAM

Online CSAM covers a wide range of behaviours and crimes, which include, but are not limited to: online grooming, exposure to online pornography, online-facilitated child sexual exploitation, production and distribution of illegal child sexual abuse imagery and the production, consumption and dissemination of such images and videos. Behind each of these crimes is a child who has been, or is being, harmed and abused. Survivors are condemned to the risk of repeated re-victimisation, violation and degradation each time their abuse is viewed. The knowledge that their abuse has been recorded, that photos or videos of it are being circulated, are out of their control and may remain online forever, contribute to and exacerbate the ongoing trauma they face.[2]

'The abuse stops and at some point also the fear for abuse; the fear for the material never ends.'[3]

'The experiences are over. I can get a certain measure of control over those experiences. With regard to the imagery, I'm powerless. I can't get any control. The images are out there.'[4]

The true scale of online CSAM is currently not known, but the fact that very young, prepubescent children are being abused and subjected to extreme sexual assaults is undisputed. Cybertip.ca analysis reported that 78% of the images and videos assessed by their team depicted children under 12 years of age, with 50% of the materials involving explicit sexual activity or assaults and extreme sexual assaults.[5]

The Internet Watch Foundation (IWF) reported that of the 80,318 confirmed reports of child sexual abuse imagery processed in 2017, 55% were of children appearing to be aged 0-10, with almost half of the children depicted in that volume subjected to the most extreme forms of abuse.[6]

Findings into the prevalence, scale and nature of these offences has repeatedly indicated that online child sexual abuse crimes are a growing phenomenon globally. More than 27 million images have been reviewed by the U.S. National Center for Missing and Exploited Children since 1998. The IWF reports that it assesses a webpage every four minutes, and that every seven minutes the webpage reviewed shows a child being sexually abused.[7]

Technology, and its ubiquity, has had a multifaceted impact in relation to online child sexual abuse material. Reports of CSAM have been found to rise commensurate

1 Chair: Julie Inman-Grant; Members: Baroness Beeban Kidron, Baroness Joanna Shields, Brooke Istook, Christian Berg, Jacqueline Beauchere, John Carr, John Stix, Peter Mackay

2 Hamilton-Giachritsis, C., Hanson, E., Whittle, H., Beech, A., 2017. 'Everyone deserves to be happy: A mixed methods study exploring how online and offline child sexual abuse impact young people and how professionals respond to it.'

3 Survivor quote from the Canadian Centre for Child Protection Inc. 2017. 'Survivor Survey: Final Report'

4 Ibid.

5 Canadian Centre for Child Protection Inc. 2016. 'Child Sexual Abuse Images on the Internet: a Cybertip.ca Analysis'.

6 Internet Watch Foundation, 2017. 'Annual Report 2017'.

7 Ibid.

with access, uptake, interaction and use of the internet.[8] It has also transformed the ability of offenders to access, control, manipulate, share, discuss, plan, co-ordinate and facilitate online child sexual abuse. For victims and survivors, it can trap them in an inescapable and manipulated environment, where the power dynamic is weighted heavily to the offender who can blackmail, threaten, coerce and control them 24/7.[9]

In 2017, INHOPE member hotlines traced the hosting of CSAM to more than 70 countries.[10] Survivors of this exploitation have been located in all quarters of the globe, with numbers of victims rising quickly in emerging technology markets and where internet access is growing the most rapidly. Research has highlighted the complexity of online child sexual abuse: there is no 'typical' offender, victim, or type of offence. Indeed, the rise in self-produced child sexual abuse content[11] and the scale and nature of peer-on-peer abuse has been a stark reminder of the ever-evolving nature of this multi-faceted and multi-dimensional crime. What is clear, however, is the impact these crimes have on survivors, their families and the families of offenders. Survivors experience devastating emotional and physical impacts, as well as damage to their educational, employment, productivity and financial prospects.[12]

Focus of the report

There has been a considerable amount of work and activity to tackle the spread of CSAM globally. In order to catalogue the companies, tools and initiatives that are operating and delivering in some capacity to eradicate child sexual abuse imagery from the internet, a technical inventory was developed by the Child Dignity Alliance Technical Working Group. The inventory was based on members' unique knowledge and experience and, as such, is comprehensive without being exhaustive. The inventory was created to:

1. ascertain whether there were any specific areas where the working group should focus its attention
2. provide a potential resource for law enforcement agencies, relevant regulatory bodies, trusted NGOs and committed industry players.

The result was a complex matrix of tools and organisations focusing on online CSAM in some capacity. The inventory outlined the variety of companies, and governments, that have dedicated resources to develop tools to detect and report child sexual abuse imagery and, in some instances, to aid law enforcement in their investigations. While the volume of forensic analysis tools raised concerns over duplication of effort, the sparsity of victim identification tools and tools that remove images of 'lower severity' perhaps reflects the deep complexity of the challenge, as well as the changing nature and dynamics of the digital world. It is of utmost importance that technological innovations and developments both reflect and adapt to the reality of how CSAM is being produced, by whom, and how. We must acknowledge the ease with which images can be generated, adapted, manipulated and spread, and reflect on measures to address any technical, cultural or societal norms that impact on the production and distribution of this content.

In general, the inventory provided a real reminder of the siloed work that often takes place in such a complex and inter-related field. To some extent the development of different tools across jurisdictions is understandable given the patchwork of legislation and procedures that both restrict and force countries, and companies, to develop bespoke solutions that can only work in isolation, or within a limited number of jurisdictions. That said, the apparent lack of any real coordination globally—in terms of developing a comprehensive, interoperable range of tools—is of real concern. Some of these challenges are detailed in the section dealing with law and policy, below.

Recommendation: 15. Governments, governance groups and industry should support the Child Dignity Alliance and the WePROTECT Global Alliance to maintain and improve a technical inventory (a central repository of current information about tools and technologies) to assist law enforcement to investigate, identify victims and manage CSAM cases.

Collaboration, multi-stakeholder engagement, and investment in prevention strategies have been described as important central pillars supporting efforts of the global community to end CSAM. Indeed, a more 'functions-based approach' to international coordination has been recently suggested, where policy is informed by a holistic view that maximises use of all specialist stakeholders, rather than being restricted to the historic and isolated domains of the various actors involved.[13] However, we can only truly move to this

8 WePROTECT Global Alliance 2017. 'Global Threat Assessment, 2017: Working together to end the sexual exploitation of children online'.

9 Hamilton-Giachritsis, C., Hanson, E., Whittle, H., Beech, A., 2017. 'Everyone deserves to be happy: A mixed methods study exploring how online and offline child sexual abuse impact young people and how professionals respond to it.'

10 International Association of Internet Hotlines INHOPE 2017. 'Annual Report 2017'.

11 Internet Watch Foundation, 2017. 'Annual Report 2017'.

12 WePROTECT Global Alliance 2017. 'Global Threat Assessment, 2017: Working together to end the sexual exploitation of children online'.

13 Baines, V 2018. 'Online Child Sexual Exploitation: Towards an Optimal International Response'.

approach if there is a genuine will to overcome many of the technical, legal and political barriers that exist, and which are currently contributing to the piecemeal and fragmented approach to addressing this crime. The impact of technological innovation in protecting children and young people from these abuses could be hugely significant, but only if we accept and address the barriers that are currently restricting their uptake and development.

The Five Country Ministerial[14] Statement on Countering the Illicit Use of Online Spaces[15], announced in August 2018, reiterates and complements many of the issues and solutions raised in this report. It clearly states a commitment and determination for greater collaboration in tackling the threat of online child sexual exploitation and highlights the real need for both governments and industry to escalate their efforts to stop the growth of this heinous crime.

14 The Five Country Ministerial is made up of the Homeland Security, Public Safety and Immigration Ministers of Australia, Canada, New Zealand, the United Kingdom and the United States, who gather annually to collaborate on meeting common security challenges.

15 Five Country Ministerial Statement on Countering the Illicit Use of Online Spaces 2018.

Efforts, issues and identified barriers

Law Enforcement

Classification of images

Although it can never be proved, it is almost certainly the case that most instances of child sexual abuse do not result in any kind of image being made and there will be little or no connection to the internet. This paper addresses a particularly harmful dimension of child sexual abuse. On top of the harm caused by the initial sexually abusive acts, there is the harm caused by the creation and distribution of images of the abuse. This can magnify, change and massively prolong the nature of the harm done to the child depicted but also, to the extent that distribution of images encourages or helps sustain paedophilic behaviour elsewhere, it puts children around the world who are as yet unharmed, at risk of being sexually abused.

For law enforcement, a precursor to identifying and rescuing victims of child sexual abuse which has resulted in an image being made, and prosecuting offenders, is the identification of child sexual abuse material. Globally, specialist law enforcement personnel are tasked with assessing images to determine whether the individual depicted in the image is a child, and whether the image is relevant—that is, whether the image exhibits exploitation or abuse, or whether it has some other evidentiary value.

Assessing the age of those depicted

Determining the age of post-pubescent individuals is notoriously difficult. Accuracy rates, and agreement between 'coders'[16], when assessing the age of individuals at the post-pubescent development stage (i.e. 15-16 years) can be particularly low.[17] This is often exacerbated when dealing with images that depict a range of individuals from different nationalities, ethnicities and socioeconomic strata.[18] In addition, differences in legal definitions of 'minors' can also exacerbate the reliability of assessments of age, particularly when coders reside in countries with materially different laws.

A recent research report highlighted that law enforcement personnel admit to proceeding with caution in relation to 'borderline images', focusing attention instead on images which are indisputably of children.[19] This has the negative implication for some victims of ongoing sexual exploitation and abuse not being identified and rescued compared to younger children.

The development of artificial neural networks in detecting child sex abuse material on the internet has ensured that images are classified faster than ever before. Classifiers have been developed that are able to differentiate the age of victims in images to a very high degree of accuracy, and systems are being developed to create high 90th-percentile accuracy. Human accuracy rates, including reliability rates between individuals classifying images, show similar levels of accuracy.[20] While work is needed to train automated classifiers on larger data-sets, and ensure they work across nationalities and ethnicities with the same or similar degrees of accuracy, overall the speed of innovation in this space is encouraging. Developments in age assessment, driven by machine learning and artificial intelligence, may lead to greater confidence among law enforcement personnel to initiate investigations into what were previously classified as 'borderline' imagery. This will go some way to ensure that more children are correctly identified as needing to be rescued moving forward. The resultant impact on policing capacity and resourcing must be addressed alongside any advancements in technological innovations and developments.

Triage

Law enforcement seizures of CSAM frequently occur as a result of search warrants, producing hard drives and external media filled with images and videos. Often, forensic technicians triage the media in the field, and rely on tools that make use of 'hash-sets[21]' of known illegal imagery to indicate the presence of confirmed abuse material. More extensive hash-sets can make for more accurate triaging in-field, leading to more complete seizure of relevant evidence by police.

16 Coders refers to law enforcement personnel tasked with grading images. Industry often refers to these individuals as content moderator agents.

17 Kloess JA, Woodhams J, Whittle H, Grant T, Hamilton-Giachritsis CE 2017. 'The Challenges of Identifying and Classifying Child Sexual Abuse Material.

18 Mayer F, Arent T, Geserick G, Grundmann C, Lockemann U, Riepert T, Ritz-Timme S 2014. 'Age estimation based on pictures and videos presumably showing child or youth pornography'. ***International Journal of Legal Medicine***, vol. 128, pp. 649-652

19 Kloess JA, Woodhams J, Whittle H, Grant T, Hamilton-Giachritsis CE 2017. 'The Challenges of Identifying and Classifying Child Sexual Abuse Material'.

20 Ibid.

21 A hash is produced by the operation of an algorithm on an electronic file, such as a digital image. Hashing images produces a value as output, which is sometimes referred to as a digital fingerprint. A hash-set is a collection or database of hashes. Law enforcement use these unique identifiers to more easily identify 'matches' with known image and video content when conducting forensic analysis of storage devices seized during investigations.

Image severity

Law enforcement personnel are also tasked with classifying images into categories, with a variety of classification systems being used around the globe to determine the images' severity (e.g. COPINE scale, Oliver scale, Interpol International Classification Scheme, Child Exploitation Tracking System, to name a few).

Assessing the level of the 'severity' of indecency depicted in a given image can be difficult, particularly in relation to images that are highly sexualised but lack any contextual information, or do not explicitly feature penetrative or non-penetrative sexual activity. Research has pointed to the fact that there is a certain degree of subjective determination in assessing whether images are indecent, with law enforcement often relying on environmental and contextual factors to aid their assessments.[22] Indeed, knowledge of what is contained in a suspect's collection can impact an analysts' interpretation of 'lower-level' images, as can the emotional reactions that professional coders have to the material viewed.[23]

As noted earlier, investment has been made by some companies to develop image classifiers that can analyse and grade images at speeds beyond the reach of human analysts. However, classifiers are only as good as the data-sets on which they are trained. As such, there are examples of different classifiers being built around the globe by different organisations, trained on different data-sets and using different classification criteria.

The benefits of these classifiers are not in dispute. They radically reduce the amount of time law enforcement need to spend classifying images, reducing adverse wellbeing impacts on personnel, while allowing investigators to concentrate on victim identification. However, the barriers that currently exist around restrictions on data-sharing between law enforcement and industry (see, Access to data section), and even between jurisdictions, have resulted in duplication of effort, and systems that can only work in isolation. For law enforcement, the proprietary nature of existing tools often prevents digital forensic examiners from being able to use multiple tools in conjunction; no single tool addresses the entire needs of law enforcement in this space. Project VIC (see, sidebar right), has gone some way to creating efficiencies in this space through the use of a standardised classification schema that has been adopted throughout the United States.

The advantages of developing a standardised system of classification frameworks, supported by harmonised legislative regimes, are potentially substantial. Parts of the law enforcement and research communities have long-called for a universal standard, schema or taxonomy.[24]

> **Recommendation:** There should be efforts made at the supra-national level, through appropriate multilateral working groups, to implement a single standard framework for the classification of child abuse imagery. This should be adopted by, at a minimum, the 'Five Eyes' countries of Australia, the United Kingdom, Canada, New Zealand and the United States. In addition, those nations should contribute to and support development of tools allowing for the 'translation' of categories from one jurisdiction to another.

It is worth raising that the impact of online child sexual abuse imagery on victims and survivors is not commensurate to the degree of severity of the image. The pervasive nature, duration and form of the abuse, as well as the individual's relationship (both perceived and actual) to the abuser and whether there were multiple abusers all significantly impact victim and survivors' experiences.[25] A demarcation simply on the basis of severity of an image serves an injustice to victims and survivors, despite the acknowledgement of the need for law enforcement to prioritise their case-loads.

Access to data

Access by investigators to images, data and related information is critical to efforts aimed at tackling the proliferation of child sexual abuse media online. We have identified four main repositories of data and information:

1. Images or other child protection concerns captured by police during investigations; sometimes referred to as 'grey area' material.
2. Hash-databases, image-databases and image libraries that have been compiled by law enforcement, hotlines, industry and other organisations to expedite the removal of child sexual abuse images online:
    - Images and other contextual information generated by internet services operating over a range of protocols (e.g. the open web, deep web, file-sharing networks, and the dark web).

22 Kloess JA, Woodhams J, Whittle H, Grant T, Hamilton-Giachritsis CE 2017. 'The Challenges of Identifying and Classifying Child Sexual Abuse Material.

23 Loewenstein G and Lerner JS 2003. 'The role of affect in decision making'. In Davidson RJ, Scherer KR, Goldsmith HH. (Eds.), Handbook of affective sciences pp. 619-642. Oxford, UK: Oxford University Press

24 ECPAT International and Interpol 2018. 'Toward a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material'.

25 Canadian Centre for Child Protection Inc. 2017. 'Survivor Survey: Final Report'.

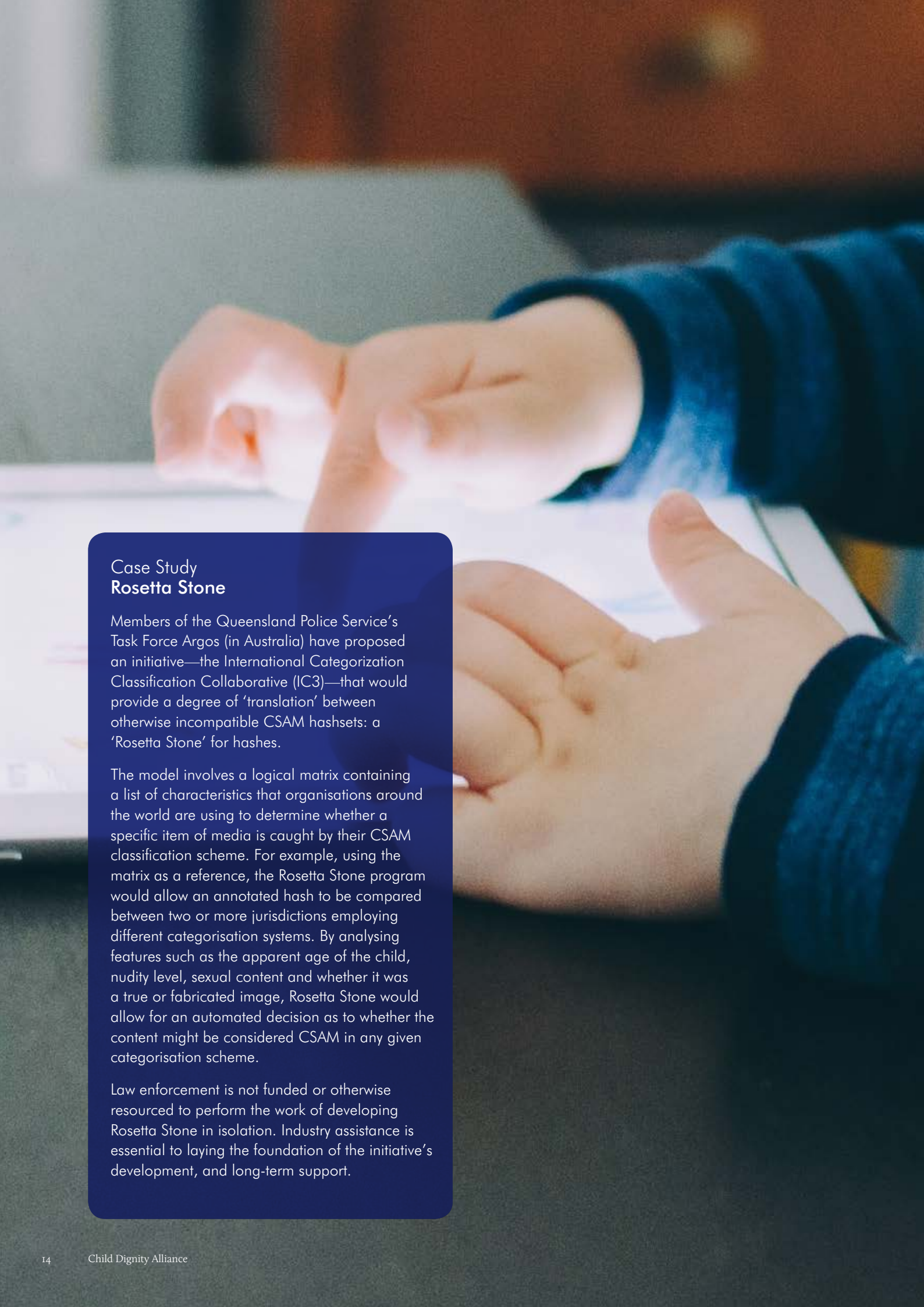
Case Study
Good Practice

Project VIC is a community of investigators, victim identification specialists, application developers, scientists and strategic partners dedicated to developing and delivering the newest technologies and victim-centric methods of investigation to improve success rates in rescuing victims of child sexual exploitation and trafficking.

It has developed a Video and Image Classification Standard (VICS), which is a data-sharing standard, using crowd sourced data-sets in the cloud that facilitate the transfer of forensic data from one software application to another in a seamless manner.

As such, huge progress has been made to reduce the siloed retention of data within law enforcement agencies, allowing agencies the ability to use collaborative data to identify 'known' images, and as a result to free up investigators' time to improve their child exploitation investigations.

The launch of VIClabs in May 2018, also highlights the intention of this project to de-conflict on issues internationally and avoid further duplication.



Case Study
Rosetta Stone

Members of the Queensland Police Service's Task Force Argos (in Australia) have proposed an initiative—the International Categorization Classification Collaborative (IC3)—that would provide a degree of 'translation' between otherwise incompatible CSAM hashsets: a 'Rosetta Stone' for hashes.

The model involves a logical matrix containing a list of characteristics that organisations around the world are using to determine whether a specific item of media is caught by their CSAM classification scheme. For example, using the matrix as a reference, the Rosetta Stone program would allow an annotated hash to be compared between two or more jurisdictions employing different categorisation systems. By analysing features such as the apparent age of the child, nudity level, sexual content and whether it was a true or fabricated image, Rosetta Stone would allow for an automated decision as to whether the content might be considered CSAM in any given categorisation scheme.

Law enforcement is not funded or otherwise resourced to perform the work of developing Rosetta Stone in isolation. Industry assistance is essential to laying the foundation of the initiative's development, and long-term support.

3. Data held by private companies and organisations:
    - Information held on servers or individual computers/devices within organisations and companies.
    - Databases compiled by companies to develop proprietary products or open-source tools.
4. Information collected by NGOs and hotlines generally gathered through reports from the general public.

Collectively, these sources provide key insights into the nature and scale of child sexual exploitation. However, there is currently limited connectivity between most of these repositories. Law enforcement are keen to harness advances in technological development to speed up investigatory processes; however, significant barriers exist about data-sharing. These include organisational, jurisdictional, domestic, legal and policy restrictions over what is considered 'intelligence data', and what can be shared with the private sector.

Evidence and research have repeatedly pointed to the fact that law enforcement agencies in many counties, including the UK, Australia, Canada and the US, are overwhelmed by the sheer volume of content that they have to investigate; that there are significant delays in the forensic analysis of digital devices; and investigations are often protracted due to heavy workloads. While some law enforcement units use technological tools developed by private entities to expedite aspects of the investigative process, the costs to acquire and maintain the tools can be prohibitive, and the tools developed may only cover certain aspects of the work.

The ability to develop, train and test algorithms and neural networks on datasets and information held by law enforcement is essential, particularly given the rapidly changing digital landscape and increasingly law enforcement-aware offenders' behavioural patterns. It has been argued that greater flexibility is needed to enable law enforcement to work more closely with trusted third-party developers to build a more holistic suite of tools that target key aspects of investigations into child sexual abuse imagery.

Historically, there have been two main types of opposition to sharing of hash data with non-law enforcement agencies. First, annotated hash data[26] has been regarded as sensitive intelligence relating to the crime of child sexual abuse and exploitation. Second, there is a sense that private companies should not be given an actual or implied commercial advantage by obtaining what amounts to exclusive access to law enforcement hash data. Both concerns impact the ability of law enforcement to innovate in collaboration with industry (see, Rosetta Stone initiative in the sidebar left.)

Recommendation: Technical data of any kind, including hash data sets, relating to child sexual exploitation and abuse imagery should be defined and treated as 'global assets'. Hashes should be made available across trusted sectors and jurisdictions to (a) aid law enforcement case management efforts (especially victim identification), and (b) assist with industry efforts to innovate and develop new identification/classification technologies.

Recommendation: To expedite investigations and accelerate innovation, industry must develop robust and universal cooperation frameworks and standards for legal interoperability for data and intelligence sharing between law enforcement agencies globally, as well as between law enforcement and trusted private entities.

The Ackerman decision of the 10th Circuit Court of Appeals

The *United States v Ackerman* is a 2016 decision of the US Tenth Circuit Court of Appeals. Following *Ackerman*, some stakeholders in the US may need to reconsider the steps they take to combat child sexual abuse imagery online if they are an 'agent of the government'. If a court finds that they are acting at the behest of the US Government, then actions such as opening emails or other forms of electronic correspondence may be deemed warrantless searches conducted in violation of the Fourth Amendment. If so, any evidence obtained may be excluded in a criminal trial. *Ackerman* ruled that the National Center for Missing and Exploited Children (NCMEC) was acting as an agent of the US Government when it opened an email purportedly containing child abuse images. To date, no court has ruled a private company to be a government agent.

Ackerman is a decision about an email sent by Walter Ackerman to persons unknown using an electronic mail service provided by AOL. Employing automated filtering technology, AOL detected the hash value of a known child sexual abuse image attached to Ackerman's email. As required by law, AOL forwarded the email and its attachments to NCMEC. A NCMEC analyst opened the email, finding several other child abuse images within. At trial, Ackerman sought to exclude the image evidence on the basis that it was derived from an unlawful

26 Image annotation is a process whereby metadata is manually assigned, in the form of captioning or key words, to a digital image or hash.

search conducted by NCMEC contrary to the Fourth Amendment. At first instance this application was denied, and Ackerman appealed.[27]

On appeal, Judges Gorsuch and Phillips, with whom Judge Hartz largely agreed, considered whether NCMEC was, in fact, bound by the Fourth Amendment. The Court held that NCMEC could be regarded as a government entity. This view was based in part on the 'special law enforcement duties and powers' NCMEC has,[28] and the effect of statutory provisions explicitly authorising NCMEC personnel to knowingly receive and review illegal material.[29]

The Court held that, even if NCMEC could not be characterised as a government entity, it should be seen as the US Government's agent.[30] As an agent of the government, a search conducted by NCMEC of papers or personal effects, including email, must be supported with a warrant to be constitutional. Their Honours found that the government 'knew of and acquiesced in' NCMEC's search, and that NCMEC performed the search with some intention to assist law enforcement. In consequence, NCMEC acted on behalf of and with the authority of the government as its agent.

Whether NCMEC's search offended against the Fourth Amendment depended on whether the tests in *Katz* and *Jones*—two Supreme Court decisions—could be made out. The principle in *Katz* holds that a search will not be a search unless some 'legitimate privacy interest' is compromised.[31] The later case of *Jones* clarified *Katz* by holding that a Fourth Amendment search will be conducted either when a reasonable expectation of privacy is violated, or when a trespass against a person, house, papers or effects is conducted in order to obtain information.[32] Through NCMEC's opening of Ackerman's email, the Court held that the tests in both *Katz* and *Jones* were met, and an unlawful search was found to have taken place.

The decision in *Ackerman* potentially renders companies working with law enforcement vulnerable to the logic applied by Judges Gorsuch and Wilson. Where the government has 'encouraged, endorsed and participated' in the actions of a private entity involved in quasi-law enforcement functions, the entity could be regarded as the government's agent.[33] If the decision is to be read in this light, the sharing of technical data such as hash values between US-based companies and law enforcement agencies is unlikely to be affected.

27 United States v. Ackerman, 831 F.3d 1292 (10th Cir. 2016) pp. 2-4.
28 Ibid, p. 7.
29 Ibid, p. 9.
30 Ibid, p. 16.
31 Ibid, p. 28.
32 Ibid, p. 32.
33 Ibid, p. 21.

Recommendation: Major technology companies like Facebook, Twitter, Google, Snap, Microsoft and others should continue to support the efforts of law enforcement, government entities and not-for-profit hotlines, including through sharing enhanced key technical and operational data, for example hash data.

Contextual evidence of child sexual exploitation

Child abuse images and videos are only one evidentiary aspect of the investigation process. In addition to the imagery itself, there is a wealth of information and data that provide a more robust and holistic picture of the crimes being conducted. Chat logs, search history, metadata from interactions online and financial transactions can all provide important information to help identify and track perpetrators and victims.

While individual law enforcement agencies capture this data when they can obtain it, it's currently unclear how much of this data is shared between national and international agencies to better coordinate criminal investigations. It's also unclear what information is passed on to agencies and hotlines dedicated to supporting and assisting victims and vulnerable groups.

Victim identification

In 2018, the End Child Prostitution and Trafficking (ECPAT) International and INTERPOL carried out a unique research project that analysed media images held in the International Child Sexual Exploitation Database (ICSE Database). The database contained over one million unique individual images and videos, with 57% of images and videos depicting unidentified children.

Of particular relevance to our report, the research highlighted the limitations of the ICSE database which was largely due to the voluntary and 'ad-hoc' nature of how it is used. Different standard operating procedures for database administration, case recording procedures and categorisation approaches have resulted in a mixed patchwork of information captured in the database.

Anecdotal evidence from law enforcement partners indicates that there is no consistent approach to annotating hashes, and there is no standardised approach to providing evidence in the form of accompanying meta-data to the hashes. There is also very little, or no, oversight over whether law enforcement agencies update the database following victim identification or other investigatory leads.

Recommendation: Leading governments, including the governments of the United States, the United Kingdom, Australia, Canada and New Zealand should support INTERPOL's planned upgrade of the ICSE database so as to (a) produce greater consistency of practice in relation to the annotation of hashes and data entry; (b) guarantee greater consistency and maintenance of data concerning identified and unidentified victims; (c) encourage greater take up of high-quality remote connections; and (d) consider additional metrics that might help identify a greater number of victims.

Innovative tools and initiatives to expedite the identification of unknown victims have been developed in both the US and Europe. The INTERPOL DevOps Technical Working Group[34] has hosted a number of hackathons focused on developing technology to combat CSAM, which in 2017 resulted in a tool that uses machine learning to triage CSAM to help LEA to quickly identify content that is most important to find new child victims. In addition, NCMEC and INTERPOL both use mobile labs, which allow law enforcement personnel, prosecutors and social service workers to access redacted and sanitised CSAM to help identify and rescue unknown child victims. These labs are deployed at events and conferences where frontline professionals gather. In addition, Europol have launched a 'Trace an Object' initiative, and the Exchange Initiative a 'TraffickCam'; the former calling on members of the public to provide tips and information about key objects in child abuse imagery, the latter requesting images of hotel rooms to assist LEA in identifying locations in child sex trafficking cases. Awareness of these labs and tools, and deployment of them globally, could significantly aid law enforcement in identifying and rescuing victims.

Online grooming

The digital world poses a range of threats and challenges to children, including online sexual grooming by predators. There are various routes through which children can be contacted by those with nefarious intent, and evolving and emerging technologies mean that there are new and very private mechanisms available to perpetuate the grooming process. In addition, extensive digital 'footprints' left online by children help predators to immerse themselves in much of the child's life as a precursor to making contact. The perennial nature of online life can create a sense of inescapability for the child victim, and total control for the perpetrator.

Recent reports have highlighted that law enforcement workloads have significantly increased as a result of developments in technology.[35] In the UK, it has been reported that the internet was used every day in 2015 to commit an average of eight sexual crimes against children, including rape, grooming, and live streaming of abuse.[36] In relation to CSAM, investigators report that the use of apps and chatrooms by offenders to both liaise with other offenders, and to coerce and force children and young people to send images and videos is increasing. Due to the hidden nature of grooming, it can be difficult to develop a clear picture of the extent of grooming, or the typical ensuing sexual exploitation.

The role of 'self-produced' sexual exploitation imagery featuring youth is a relatively recent phenomena and is being flagged as a cause for concern among law enforcement—in particular the volume of content that is being produced and uploaded online. It's important to remember that online grooming is typically a covert operation, one that centres on befriending and gaining the trust of the victims, which means it can be a very difficult process to interpret until a notable boundary has been crossed. For the young person in question, he or she may be so emotionally invested in the 'relationship' that he/she fails to recognise the abuse and exploitation.[37] This ambiguity makes it difficult to define and distinguish online grooming from a range of other forms of abusive behaviours, or to differentiate clearly self-generated images featuring youth that have been produced through coercion or manipulation versus self-produced indecent images as part of consensual sexual exploration. It is also important to highlight that the vast majority of child sexual abuse is carried out by those within the immediate family, or a child's 'inner circle'.[38,39]

34 The INTERPOL DevOps Technical Working Group is a sub-group of INTERPOL Specialists Group on Crimes against Children.

35 NetClean 2017. 'Eight Important Insights into Child Sexual Abuse Crimes'.

36 See https://www.theguardian.com/society/2016/jun/21/internet-used-in-eight-cases-of-child-sex-abuse-every-day-nspcc-finds

37 Whittle H, Hamilton-Giachritsis CE, Beech AR 2014. 'In their own words: Young peoples' vulnerabilities to being groomed and sexually abused online'. Psychology, vol 5, pp. 1185-1196

38 Finkelhor, D 2009. 'The prevention of childhood sexual abuse', The Future of Children, vol. 19(2), pp. 169-194.

39 UKCCIS Research Highlights for Children's Online Safety #62 February 2014.

A significant number of sexual crimes involving online sexual communication with a minor are perpetrated by other young people.[40] Research has made clear the enormous scale and prevalence with which young people are solicited online to engage in sexual discussions and to produce sexual imagery and videos. A recent survey carried out in the UK has highlighted that 1 in 25 primary school children surveyed had been sent or shown a naked or semi-naked image by an adult, and 1 in 20 by another young person[41]. The role of social media platforms and online forums acting as a gateway to online grooming and sexual solicitation has long been established,[42] as has the uploading of sexually explicit photos or videos placed on the open internet to offender 'collections'.[43,44]

Greater attention is being paid to identifying online grooming as a communicative process, and as a result research is beginning to focus on developing models of how groomers use language to build relationships with children and young people.[45,46] With these types of models in place, the development and broad deployment of technical tools to flag and surface grooming linguistic patterns will not be far behind. The capabilities of such systems, sitting alongside tools that utilise metadata to identify accounts displaying suspect behaviour could highlight concerns to young people about the person they are interacting with. Indeed, a Concept Demonstrator has recently been developed that goes some way towards doing just this.[47] A holistic approach that embeds technical solutions alongside education and awareness-raising initiatives would go some way to assisting young people in navigating the online world more safely.

For CSAM, attention to date has focused on identifying and removing imagery involving penetrative and non-penetrative sexual activity. However, online grooming is a process and, as such, a truly preventative approach should also focus on identifying the sequential pattern of images, with the aim of identifying children and young people whose images are escalating in frequency and severity, and whose images are repeatedly being accessed. Rather than waiting until a child has been subjected to sexual abuse before victim identification or child protection procedures begin, greater attention and resources could be paid to the early signs of vulnerability and risk that are captured in both meta-data and in images or videos themselves. The possibilities of new technologies in this area are largely unexplored—their greatest potential lies in identifying and escalating concerns about those being groomed to usher in intervention and support.

Microsoft recently announced a multi-pronged, cross-industry hack-a-thon looking specifically into proactive approaches into identifying and combatting online child grooming for sexual purposes. The hack-a-thon is due to take place in November 2018. In taking a multi-disciplinary approach to the hack-a-thon, Microsoft and other large tech companies hope that technological innovation can play a role in surfacing potential instances of online sexual grooming, while addressing and aiming to clarify legal and policy tensions.

Live-streaming

The live-streaming of child sexual abuse has repeatedly been identified as a key and growing threat in the area of child sexual exploitation. Concerns relate to both the profit-driven (commercial and the 'high value' currency of new material) motives of live-streaming of sexual abuse, such as live distant abuse and 'on-demand' abuse, as well as the role that live-streaming capabilities play in the grooming of children and young people for sexual exploitation and abuse[48].

The increased rate of access to the internet and to mobile devices globally, and the development of faster, cheaper and more seamless internet access infrastructures, has been considered a major factor in the growth of several forms of online child sexual exploitation material[49]. However, in its latest threat assessment, the WePROTECT Global Alliance specifically highlights the intersection of relative poverty and the widespread use of English in developing countries, to upward trends in prevalence of live-streamed abuse.

A recent study carried out by the Internet Watch Foundation (IWF) that focused solely on image and video captures of live-streamed abuse, found that the majority of imagery depicted children assessed as being aged 11-13 years of age, with 40% of the imagery being classified at the highest levels of severity[50]. None of the

40 Wolak J and Finkelhor D 2013. 'Are crimes by online predators different from crimes by sex offenders who know youth in-person?' Journal of Adolescent Health, vol.53, pp. 736-741

41 NSPCC snapshot 1 2018 'Children sending and receiving sexual messages'.

42 Europol 2018. 'Internet Organised Crime Threat Assessment'.

43 Ibid.

44 Smith S 2012. 'Study of Self-Generated Sexually Explicit Images & Videos Featuring Young People Online'.

45 Lorenzo-Dus N, Izura C, Perez-Tattam R 2016. 'Understanding grooming discourse in computer-mediated environments'. Discourse, Context & Media, vol. 12, pp. 40-50.

46 Lorenzo-Dus N, Izura C 2017. '"cause ur special": Understanding trust and complimenting behaviour in online grooming discourse'. Journal of Pragmatics, vol 112, pp. 68-82.

47 Please see: https://www.paconsulting.com/insights/protecting-children-from-online-sexual-exploitation-and-abuse/

48 Europol 2018. 'Internet Organised Crime Threat Assessment'.

49 WePROTECT Global Alliance 2017. 'Global Threat Assessment, 2017: Working together to end the sexual exploitation of children online'.

50 Internet Watch Foundation 2018. 'Trends in Online Child Sexual Exploitation: Examining the Distribution of Captures of Live-streamed Child Sexual Abuse'.

imagery included the physical presence of an adult, with most children recorded as being alone in their bedroom or bathroom. This should not be read as implying that the child was not being manipulated by a third party, either a peer or an adult. Indeed, the report specifically highlights children being coerced into producing imagery in the form of a 'game of likes', with young people agreeing to engage in activities in return for rewards, most commonly 'likes' or comments. All of the images had been harvested from their original upload location and were being distributed via third-party websites.

Live streaming of child sexual abuse creates significant challenges for intervention and for law enforcement investigations. The use of strong encryption is also a common feature of the live streaming system so unless an offender records the broadcast, or captures images from the live-streamed abuse, there is likely to be little trace of the abuse and who was involved. It is imperative that greater attention is paid to those who utilise live-streaming platforms to generate, distribute and share child sexual abuse materials, as well as to proactively identify and take action against illegal content in real time in terms of victim identification and removal of content. There may also be scope for greater co-operation with payments service providers to help identify the financial flows which are typically related to live streaming.

Industry

The role of industry in developing tools to detect and expedite the removal of CSAM; to report to relevant authorities perpetrators who share and distribute illegal material on their platforms; and to help citizens more safely navigate the online world, is critical[51].

There are numerous examples of successful innovations by industry in this area, including the development of PhotoDNA and other robust hash-matching, webcrawlers, video fingerprinting, investigatory toolkits, visual intelligence tools, image classifiers and hash databases to name but a few. The sheer range of organisations and companies dedicated to assisting with victim identification and addressing the proliferation of CSAM is heartening. Such developments should be encouraged, supported and promoted. They should also be better coordinated, and the licensing processes more streamlined, so as to avoid duplication, encourage uptake and to ensure that the most critical aspects aiding proliferation of images are addressed. Through these measures, many of the drivers of demand for this type of material will be reduced.

The recent announcements by both Google and Facebook on the development of new technologies and toolkits to help organisations review, report and prioritise CSAM at speed, while also reducing the need for human inspection, are phenomenal steps forward. The news that Google's toolkit will be released for free to NGOs and industry partners is welcomed; however, the TWG would like to see positive steps also to share the technology with relevant government regulators and law enforcement agencies on the frontline. Facebook's proactive technology to detect child nudity and previously unknown child exploitation content when it is being uploaded, highlight the true potential of advancements in machine learning and artificial intelligence. The possible impacts that these, and other technologies that have also been developed by others, will have on expediting the identification of victims, the erasure of material, and eradicating CSAM online is truly significant.

Recommendation: Industry must work collectively to reduce the siloed and fragmented patchwork approach to the development of technical tools such as AI classifiers and hashing algorithms. It must be a guiding principle that technology which tackles child sexual abuse imagery is shared, standardised and placed at the disposal of all parties involved in fighting against this crime, regardless of sector.

Role in addressing CSAM on online services and platforms

We have seen the impact of a proactive approach to CSAM made by some companies, including through the use of PhotoDNA and PhotoDNA for Video hashing systems, Video ID software, website blocking, and the filtering and classification of search queries relating to child sexual abuse. While all major internet companies should report CSAM to the relevant law enforcement or child abuse image hotline in their jurisdictions, this is not a universal practice, even when compelled by law.

It is essential that the best tools, measures and safeguards are in place to help and support children and young people navigate the online world safely. Such safeguards should also ensure that those trying to harm or place our children at risk are prevented, deterred or interdicted before any real damage has been done. As such, it is imperative that the expectation or duty to report suspected cases of child sexual exploitation, in all its forms, is addressed by industry at large.

NCMEC's CyberTipline is a centralised reporting mechanism for the US public, NGO's and electronic service providers to report suspected child sexual exploitation. Currently more than 1,500 US electronic service providers have access to the reporting mechanism. From CyberTipline reports, NCMEC derives and shares more than 1.6 million child sexual abuse image hash values with industry as part of a voluntary initiative to ensure that platforms can help reduce the proliferation of child sexual abuse images online. More than 27 million reports of suspected child sexual exploitation have been made to the CyberTipline between 1998 and 2017[52]. In 2017, US-based electronic service providers submitted 99% of those reports to CyberTipline, 93% of which involved individuals outside of the country uploading CSAM onto a US providers network[53]. As a result, NCMEC has evolved into a global clearinghouse on child sexual exploitation matters and makes CyberTipline reports available to US law enforcement and more than 100 international law enforcement agencies. NCMEC also partners with INTERPOL to disseminate elements of CyberTipline reports to any country not covered via NCMEC's direct referral system. The IWF, the UK's hotline, identifies only 130 global companies currently working to make the internet safer through the foundation's member services. This is set against the backdrop of more than

51 Please refer to the WePROTECT Model National Response for an overview of industry responsibilities: WePROTECT Global Alliance 2016. 'Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response'.

52 See https://www.cybertip.ca/app/en/

53 Statistics provided to the Child Dignity Alliance Technical Working Group from NCMEC September 2018.

351,000 ICT businesses registered in the UK in 2017.[54] It is essential that there is greater adoption of existing tools to identify and take down CSAM by all in the technology industry. The mature members of the IT industry who are already reporting could play a more active leadership and facilitative role, supporting smaller industry partners in adopting these technologies and taking an increasingly active stance in the fight against child sexual exploitation.

In order to adopt a proactive approach to the detection and removal of child sexual abuse images, industry at large needs to be aware of the nature and scale of risks on their services and platforms. For many organisations, awareness of the types of illegal and harmful behaviours that could occur on their platforms or on their equipment, is low. There is increasing momentum globally to ensure that user-safety is embedded into the design and functionality of online services and platforms from the earliest stages of development, and individual countries are in the process of developing safety-by-design frameworks and principles to assist industry in achieving best practice in this (see Office of the eSafety Commissioner in Australia). The importance of prioritising the protection of users by building user safety into online platforms and services was one of the calls made to industry at the recent Five Countries Ministerial meeting. Greater attention is also being paid to the importance of age-appropriate design of services (see UK's Information Commission Office Age Appropriate Design Code). Globally, industry is being called on to design their systems and processes with the needs of children and young people in mind, acknowledging that children merit specific protections in the digital world, just as they do offline.

Recommendation: To ensure that predators are not exploiting online services to groom and abuse children, owners of interactive platforms and services should make better use of the data they collect about their users. This will enable them to proactively identify threat actors and vulnerable users—especially children—and ensure measures are in place to allow swift and effective intervention, disruption and support.

There are other examples of initiatives trying to address the role that industry can play in addressing this crime. In 2015, the Technology Coalition developed a guidebook[55] for handling child sexual exploitation images, and Thorn, an international anti-child sex trafficking organisation, published a 'Sound Practices Guide' in the same year. The Thorn guide educates companies about proven practices, tools and resources that exist to identify, remove, report and prevent CSAM and abusive behaviour. This guide is currently being updated, alongside a practical toolkit targeting SMEs. The TWG is keen to help promote both of these resources and assist more industry players to play an active role in tackling this crime, including through the assistance of government within their home jurisdictions.

Recommendation: Governments should require industry to develop procedures that ensure CSAM on their networks is detected, reported and speedily removed. This will require legislative and policy clarity about industry's obligations, penalties for non-compliance, and the development of guidance, information and resources to aid and assist industry to comply.

In addition, innovative tools that aim to proactively reduce the online availability of CSAM and videos globally, such as Project Arachnid, have the potential to radically alter the landscape. While initially developed to crawl sites previously reported to Cybertip.ca, it now also has an application programming interface (API) for electronic service providers to crawl their systems. This both improves upon and accelerates the detection of harmful material—if industry deploys the tool.[56] Again, it is imperative that industry is encouraged, or possibly even required through legislation, to utilise tools such as this.

54 House of Commons Library 2017. 'Briefing Paper. Number 06152, 28 December 2017: Business statistics'.

55 The Technology Coalition 2015. ' Employee resilience guidebook for handling child sexual abuse images'.

56 See https://www.cybertip.ca/app/en/projects-arachnid

Recommendation: Industry should be strongly encouraged, or even required through domestic legislation, to (a) adopt PhotoDNA and PhotoDNA for Video or other child sexual exploitation and abuse material identification and sharing technologies; (b) be required to scan their networks, platforms and services, or take similar active measures, as a default operating procedure, to detect known child sexual abuse imagery content, including so-called 'passthrough' services; (c) enforce standards and codes of conduct against illegal behaviour on their platforms; and (d) implement Safety by Design frameworks, codes of practice or minimum standards.

Development of bespoke tools

Some industry players use the wealth of information and data that they hold on their platforms to develop bespoke tools (i.e. tools developed solely for use on their platforms) to combat illegal behaviour on their services. These tools are most commonly proprietary, as user-safety is often considered a 'commercial advantage' to some players. In the case of CSAM and related behaviours, this technology must be shared.

The potential for technological innovation in uncovering sequential patterns of behaviour and other indicators that could lead to better identification of higher-risk offenders and locating vulnerable individuals caught within the complex web of online sexual exploitation, is currently largely untapped. Indeed, in better identifying patterns of grooming and exploitation on interactive platforms, tech companies could provide the key to the development of robust preventative solutions to these crimes. International laws should allow for the data collected or produced by the tools to be integrated with global collaborative platforms for the use of LEA in child exploitation and trafficking cases.

Intelligence-sharing

Collaborative information and intelligence-sharing among industry players is not widespread. An important exception to this is PhotoDNA, developed to improve and expedite the identification, removal and reporting of child abuse images across different platforms and online services. The TWG acknowledges it is essential that the security and integrity of these shared hash databases are maintained.

Other types of information, for example accounts, profiles and usernames, that have been removed or blocked from individual platforms and services for engaging in child sexual exploitation activity, are not currently shared with other industry players.[57] As such, while one platform may have reported an account to law enforcement for investigation, there is currently no system in place that identifies whether that individual's profile and details are present on other interactive platforms—and therefore is able to continue to abuse victims on other sites. It would be worth exploring whether similar intelligence-sharing capabilities could be developed to be able to cross-relate intelligence and users across different platforms to better target high-risk offenders and expedite the identification of victims. A clarification of Terms of Use and Memorandums of Understanding between companies, and between companies and their users, could go some way to allow this kind of inter-company sharing to take place.

Industry players and law enforcement have a wealth of data on their systems that at present is siloed and often not used for research purposes, particularly in the preventative space. The creation of a central repository of data, or more collaborative intelligence-sharing practices, would help to provide key stakeholders with a more accurate understanding of how to tackle this issue, how to share best practice and to consider ways to provide less opportunity for individuals to engage in online child sexual exploitation. We acknowledge that within existing legal and policy constraints, particularly in relation to US Fourth Amendment, that this solution is currently untenable.

Recommendation: The technology industry should work collaboratively and exchange operational data and intelligence about those abusing their networks to share and distribute child sexual abuse imagery. Part of this might include larger companies providing more formalised and systematic support against child sexual abuse imagery to smaller industry members as part of an 'industry leadership' role.

57 A trial system of inter-company sharing was in place in 2016, but ceased following the ***Ackerman*** decision.

Legal and policy

Internet governance

Internet governance refers to the rules, policies, standards and practices that seek to coordinate and shape global cyberspace. Addressing governance and compliance issues is central to making progress in better protecting children online. Unfortunately, despite the fact that children and young people are significant stakeholders, they have been vastly under-represented and their interests unarticulated in internet governance forums. This can be attributed in no small measure to the resources, particularly financial, required to attend and engage in these multi-stakeholder events. The consequences of this absence of children's voices, or their advocates, in these critical debates have been numerous.

Of particular relevance to this paper are the lack of robust governance and compliance standards enforced by the Internet Corporation for Assigned Names and Numbers (ICANN). ICANN's Registry Agreement fails to include even the most rudimentary safeguards to protect children and young people in the creation and maintenance of Generic Top Level Domains (gTLDs). A stark example, is the process that was undertaken to award the contract for a .kids Registry. ICANN has acknowledged that they did not seek, obtain or consider any expert advice in relation to what would be in the best interests of children online. Neither were any extra or specific requirements imposed within the application or assessment processes used to decide who might become the .kids Registry. Set against the pre-approval processes which were established before domains are awarded for the banking, insurance and pharmaceutical industries, the lack of measures undertaken in relation to children's interests is incomprehensible.

On a more positive note, the Council of Europe recently set out clear recommendations about measures to be adopted by the Registries of country code top level domains with a view to protecting children's interests. These measures should be taken up by every type of top level domain. The recommendations include due diligence requirements and the need for appropriate child-protection policies to be put in place when selling domains which are likely to appeal to children. In the interest of international cooperation and coordination, it would be opportune for the global community to consider adopting similar, or aligned, recommendations.

Another major concern is the continuing high level of inaccuracy in the WHOIS database. Ultimately this is the responsibility of ICANN[58]. In 2011, the WHOIS policy review team[59] identified that only 23% of all the WHOIS data were wholly and completely accurate, and 21.6% were so defective the data rendered the owner unreachable. In the case of CSAM, the accuracy of this database is essential to contact domain owners to inform them that illegal content is on their site, and to take steps to remove it expediently. It is imperative that ICANN enforces its contractual terms in relation to breaches of contracts which require WHOIS data to be accurate. As context, in 2018 the IWF reported that around 70% of all CSAM reported to it in 2017 was found within .com and .net, both of which are owned by the same company, Verisign, based in Virginia. If the ownership and management details of every .com and .net web site owner had been robustly verified it is highly unlikely patterns of this kind would be repeated.

To compound the problem, the benefits of a centralised and reliable database of website and domain name owners were not considered when changes to data protection legislation started in the late 1990's. Data protection and privacy were absent in any consideration of the public interest benefits of maintaining an accurate database for the purpose of locating owners whose domain names were being used for illegal purposes. Setting aside issues of what information is made publicly available, or on what basis law enforcement might access WHOIS data, the need for WHOIS data to be accurate is surely indisputable.

Recommendation: Internet governance bodies, including ICANN and registry operators such as Verisign, must take robust and transparent steps to improve the verification of customer identity when new domains are registered or renewed. They must also ensure that those representing and advocating for children's rights are fairly and robustly represented in their fora.

58 The WHOIS database was set up in order to ensure that an accurate record was made of the name, address and contact addresses of the individuals or entities who owned, or were responsible for the management of, web sites or domains.

59 WHOIS 2012. 'WHOIS Policy Review Team Final Report'.

International instruments

There are key international frameworks, conventions and instruments that define international standards for protecting children and young people online, and in combatting online child sexual abuse and exploitation.[60] The creation of global alliances (such as WePROTECT, Council of Europe, Lanzarote and Budapest Conventions and the Child Dignity Alliance) go some way to align nations within an overarching objective to tackle online child sexual exploitation. International agreements have also led to greater cooperation and the involvement of international law enforcement agencies, namely INTERPOL, Europol and the Virtual Global Taskforce.

While these instruments and alliances are vital to describing norms and encapsulating a political and moral consensus to protect young people from online exploitation, there are still significant barriers around differences in national implementation, legislation and engagement.

Many countries have not signed or ratified applicable international conventions or instruments. Further, according to the International Centre for Missing and Exploited Children (ICMEC)[61], a substantial number of countries (35) have no legislation that specifically addresses online child sexual abuse images. In addition, of those countries that do have legislation in place, 76% do not define CSAM, and only 37% of the countries criminalise possession, regardless of intent to distribute. As such, there are jurisdictions in which individuals can readily evade the reach of law enforcement.

To add to the complexity, within countries that do have legislation which addresses this crime, significant differences nevertheless continue to exist between national jurisdictions—most commonly via differing definitions and terminology used within criminal codes. In addition, given the rate of technological innovation, criminal codes can also soon fall behind how technology is used to facilitate crimes. Because of this, legislation may not reflect the reality of what is happening on the ground.

The development of universal and consistent definitions and terminology of online child sexual abuse and exploitation—and all its manifestations—is essential. Disparate and disjointed national legislation needs to be harmonised in order to strengthen cooperation and collaboration between and among countries, so that we can truly begin to make a difference in this space.

Recommendation: Governments, through the Child Dignity Alliance and the WePROTECT Global Alliance, should immediately commence work on ensuring that their domestic legislative frameworks comply with the International Centre for Missing and Exploited Children's Model Legislation; and that consistent definitions and terminology are adopted alongside these efforts that are consistent with the 'Luxembourg Guidelines'.

If we look at how online tech industries traverse the legislative patchwork that exists around the world when trying to deliver services to global citizens, we find a complex web of community standards, protocols and systems in place. While many of the major companies have formed, or are part of, global networks and initiatives that are developing their own frameworks to protect and advance the rights of users in the digital world, it's important that an artificial separation of responsibilities, endorsement and obligations under universal human rights does not take place. Indeed, there is a line of jurisprudential reasoning which holds that businesses residing in States that have ratified international instruments are themselves bound to implement provisions and should be bound to enforcement of their duties therein[62]. Alternatively, it falls to States to ensure the provisions are being met.

Recommendation: Global frameworks that are established to advance these recommendations should embody child sexual abuse imagery efforts and human rights obligations, while balancing the need to maintain standards of privacy, security and safety.

Extraterritorial legislation

A key difficulty in enforcement of cross jurisdictional offences is the 'double criminality' prerequisite for prosecution and extradition, which means that the conduct must be criminalised in both the home country of the perpetrator, and in the home country where the offence occurred. As highlighted above, many countries still do not have legislation to address online child sexual exploitation, and so perpetrators can rely on the double criminality defence and continue their abuse without fear of legal response.

60 The Optional Protocol to the (UN) Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography; the Convention on Cybercrime; and the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse.

61 ICMEC are due to release an update to this report in the imminent future.

62 United Nations Human Rights, Office of the High Commissioner 2011. ' Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework'.

This points to the need for consistent and universal terminology and definitions of online child sexual exploitation and abuse, and the development of harmonised, robust and comprehensive global legal frameworks.

Emerging technologies

Online CSAM is being shared in a multitude of ways that were not conceived of a few years ago. As outlined, the live-streaming of abuse, 'abuse-to-order' and youth self-produced sexual imagery are some such examples, as is the presence of material on distributed ledger systems. The advent of encryption; alternate, mixed, virtual and augmented reality; decentralisation of the web and quantum computing will, and indeed are already, impacting on the manifestations of online child sexual abuse and how material is spread and consumed.

How legislation and law enforcement can keep up with, and adapt to, the role of emerging technologies is essential to consider in this space. It is imperative to ensure that legislative frameworks are flexible and adaptable in order for law enforcement to be able to respond to emerging technologies that shape and change the social and criminal environment. In addition, it is vital that digital technologies are built with user-safety in mind, and that risks and harms are considered and addressed before a product is taken to market. Evidence of the steps taken to mitigate against the spread of abusive images and behaviours must be considered in the context of legislative and regulatory changes that are being discussed globally.

Intersection of privacy, security and safety

The advent of new data protection and privacy legislation has raised concerns about how legislation such as the General Data Protection Regulation (GDPR) intersects with the European Privacy Regulations (ePR) and the European Commission's recommendation on measures to effectively tackle illegal content online.

In relation to the ePR, Article 5 prohibits the processing of data unless consent is given by the end user. No exemptions exist under the regulation, and as such, companies would not be able to proactively use existing technologies to identify child abuse images unless all users consent to data processing. This is somewhat contradictory to the EU recommendation in the latter Recommendation, which outlines the important role that 'proportionate and specific proactive measures taken voluntarily by hosting service providers' can have in tackling illegal content online. To obfuscate matters further, in order to comply with GDPR legislation, companies need to have a legal basis for processing personal data. If there is no legal basis, or where the legal status of content is not harmonised between countries, industry may be unable to proactively search and flag this type of behaviour. The legitimate interests grounded in one piece of legislation may therefore be overridden by the interests or fundamental rights of data subjects within another piece of legislation.

Principles of safety, security and privacy should be complementary, not mutually exclusive, and must be balanced with one another by necessity. In relation to child abuse images online, there ought to be no room for doubt or ambiguity on whether industry is able to utilise existing technical tools to eradicate the internet of illegal content.

Further, Section 230 of the US Communications Decency Act shields internet services and technology companies from liability based on a third party's content in subsection (c)(1), stating: 'No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.' While some believe that Section 230 has been one of the most important provisions protecting free speech online, others believe that the liability protections are too broad, acting as an unmeasured defensive shield against a wide range of online ills. The technology industry has been pressing for legislative 'safe harbours' from liability through national legislation and even bilateral trade agreements. Globally, pressure has been placed on ensuring that online services and platforms are held to account for the content on their platforms. Once a provider is made aware of illegal content, either via public reporting or via active detection, it should be that platform's legal and ethical duty to remove it, or to take reasonable and proportionate steps to seek to remove it. Industry should not be held liable for content that was not surfaced or flagged to them via these means. They should however, be encouraged to do more to monitor their networks for illegal and harmful content directly. Indeed, if safe-harbour protections were afforded in more jurisdictions, perhaps more companies, especially non-US industry actors, would be willing to take a more active role in detecting and removing CSAM from their services.

Recommendation: Governments should, to the greatest extent possible, and being respectful of legitimate privacy rights, remove any doubt or ambiguity about the legality of internet businesses deploying technical tools in the fight against CSAM.

Information-sharing

Criminal investigations in general, and particularly those into online child sexual exploitation and abuse, require access to evidence that is often stored by private companies. This is increasingly in the cloud, and in jurisdictions outside that of the requesting law enforcement agency. To date, there have been limited procedural guarantees that law enforcement will be provided with the requested information in a timely manner, and in some jurisdictions direct requests are not even allowed. Anecdotal accounts have been provided to the TWG Secretariat by Australia LEA about policy directives made in overseas jurisdictions that have significantly impeded the exchange of case intelligence. These directives prohibit national LEA from sharing subscriber information about child sex offenders using certain social media services unless a request is furnished under the Mutual Legal Assistance Treaty (MLAT) process. As our colleagues have noted, 'Using MLAT to obtain subscriber information is a totally unworkable situation when we need to identity child sex offenders ASAP.' Investigating judges in Holland have reported that they have abandoned MLAT altogether because it has 'never' resulted in them acquiring any information which they could use.

There is an urgent need for the development of policy standards, regimes and processes that clearly define the conditions under which law enforcement agencies can request and access data and information held by private entities. The Internet & Jurisdiction Policy Network, in its 'Ottawa Roadmap', is seeking to tackle these issues under their data and jurisdiction programme.

Information governance around CSAM, and cybercrime in general, is currently maintained at a national level. As indicated earlier, debates are ongoing as to whether data relating to CSAM should be a 'global asset' and thus not restricted to use by a single jurisdiction or agency.

In order for law enforcement globally to be able to work more collaboratively, the effective sharing and coordination of national data analytics capabilities needs to be addressed. At present, legislative frameworks across different countries and within jurisdictions place inconsistent, unhelpful and arguably arbitrary restrictions on information use and sharing which impede information-sharing and technological innovation.

The development of a cooperation framework and standards for legal interoperability for information-sharing between law enforcement agencies would go some way toward breaking down existing barriers. In June 2017, the Council of Europe Convention on Cybercrime Committee agreed to develop a Second Additional Protocol to the Cybercrime Convention covering trans-border access to data. The Protocol seeks to establish more effective formal mutual legal assistance between countries, establish informal cooperation mechanisms, provide a framework for direct cooperation with service providers, and provide a basis for trans-border access to data by law enforcement. The Five Country Ministerial that took place this year reaffirmed a commitment to sharing criminal and law enforcement information in order to support more effective responses to serious criminal threats.

The enactment of the Clarifying Lawful Overseas Use of Data Act (CLOUD Act) in the US provides processes and procedures for US law enforcement to make requests for data in other countries. In addition, it also allows certain foreign governments to enter into new bilateral agreements with the US, under which providers could disclose data directly to the government in the other jurisdiction for serious criminal investigations. Such arrangements would go some way to expedite investigations, however disparate agreements are not universal and add to, rather than streamline, the existing complex tapestry of legal arrangements. As such, they are far from ideal in trying to establish a universal and global approach to tackling child sexual exploitation and abuse online.

Conclusion

The Child Dignity Alliance Technical Working Group set the goal of seeking to identify and harness technical innovations that would have a significant impact on CSAM. It was clear from the first meeting that there are numerous barriers that have hindered, or at least slowed, progress globally on eradicating the proliferation of CSAM online. The group felt that until these barriers had been exposed and resolved, the potential of technological development and the ability to truly harness and promote innovation, investment and commitment among the global community, was severely limited.

The normative forces that determine and guide the development of the digital world are digital governance and digital regulation—both of which should be guided by an overarching framework of digital ethics. It is the role of digital ethics to shape policies, procedures and standards for the digital world, as well as the specific legislation and rules by which the digital world is run. The ethical duty to preserve the rights and dignity of children and protect them from abuse and exploitation is relatively undisputed. As such, we need to capitalise on this shared ethical foundation to shape and direct a more standardised and co-ordinated approach to the governance and 'regulation' of online child sexual abuse and exploitation

This report has attempted to highlight some of the barriers that exist, as well as allude to positive developments that could assist in breaking down silos, while tackling fragmented approaches and restrictive policies and procedures. Two themes have emerged. First, the need for greater standardisation of process, practice and policies; second, the need for greater collaboration, coordination and inter-operability across stakeholders and functions, nations and jurisdictions.

1. Standardisation

Greater consistency in how online child sexual abuse and exploitation is defined and legislated against globally, would allow for the development of a harmonised, robust and comprehensive global legal framework. The development and adoption of universal and consistent definitions and criminal provisions relating to child exploitation and grooming would go some way to align legislation globally and help unify the international community in tackling this crime.

For law enforcement, there is a real need for the development of universal and open standards for categorising and capturing evidential aspects of CSAM. Law enforcement has long advocated for the need to develop and test a global system of analysing, identifying and classifying images that is standardised and truly cross-jurisdictional in nature. The development of this system alongside the development of standard operating procedures for evidence-capture, recording and database management by law enforcement, hotlines and private entities would provide the global community with a robust and comprehensive system for investigating these crimes.

There is also a need to secure an industry-wide commitment to take action against CSAM online. Placing a duty on industry to use existing tools to identify and remove CSAM from their services, enforce against illegal behaviour on their platforms and innovate to prevent upload of this content is one route that is gaining traction globally, namely through Safety by Design frameworks, codes of practice or minimum standards. Clarifying the expectation or duty for industry at large to report and tackle child sexual exploitation is important and ensuring that existing tools and features are implemented in accordance with the law is essential. The development of guidance and resources to aid and assist industry in this regard is a welcome step, and these products need to be widely disseminated and publicised.

2. Co-ordinating and maximising effort

Data relating to child sexual abuse and exploitation must be seen as a 'global asset', and not unnecessarily restricted to a single jurisdiction, agency or function. Existing restrictions on information use and data-sharing capabilities currently seriously impede the swift identification of victims, and how these crimes are investigated, and so the effective sharing, storing and coordination of data, intelligence and best practice is an area that needs to be seriously addressed. The development of cooperation frameworks and standards for legal interoperability between law enforcement agencies globally, and between law enforcement and trusted private entities is also vital. So too is the provision of robust processes and procedures for law enforcement to have trans-border access to data for serious criminal investigations.

While tensions exist as to the role that private corporations should play in cooperating and assisting law enforcement in their investigations, the role of industry in helping law enforcement and governments to develop tools to combat online child sexual abuse and expedite criminal investigations is indisputable.

Measures to ensure that trusted industry partners can access LEA datasets and information in order to test, train and adopt advances in machine learning and artificial intelligence is essential if we are to harness the true potential of technological innovation to combat these crimes. The creation of a global repository of data and information and a global collective of industry partners to work centrally on developing universal tools would go some way to assist in maximising and coordinating efforts.

There is also a role for industry to play in the sharing of intelligence and communications across different technology platforms to better target high-risk offenders and expedite the identification of victims. The development of intelligence-sharing capabilities among industry members would be advantageous for this, as would clarifying legal processes to allow industry to collaborate more effectively and efficiently in removing content and accounts used to sexually abuse or exploit children.

Additionally, interactive platforms and services are host to an enormous amount of data and information that could be used to assist in the development of models and indicators to better identify higher-risk offenders and vulnerable individuals caught within the complex web of online child sexual exploitation and abuse. Centralised access to communication and online data signals held by online platforms and services could revolutionise the development of preventative and interventionalist solutions to online child sexual exploitation and abuse. Interoperability, data and information-sharing are all key to radically transforming how child sexual exploitation online can be tackled. A strategic approach for how we can best utilise the wealth of data and information that exists within different organisations, agencies and countries is required. In addition, we need to ensure that industry members globally are aware of, and use, the existing tools and resources to tackle this crime, and are encouraged to innovate further so that we can truly move forward in protecting children and young people from these most heinous crimes.

Main sources

Baines, V 2018. 'Online Child Sexual Exploitation: Towards an Optimal International Response'. Retrieved from https://www.ecteg.eu/online-child-sexual-exploitation-towards-an-optimal-international-response/

Canadian Centre for Child Protection Inc. 2016. 'Child Sexual Abuse Images on the Internet: a Cybertip.ca Analysis'. Retrieved from https://www.cybertip.ca/pdfs/CTIP_CSAResearchReport_2016_en.pdf

Canadian Centre for Child Protection Inc. 2017. 'Survivor Survey: Final Report' Retrieved from https://www.nationaalrapporteur.nl/binaries/Executive_Summary_Survivors%27_Survey_tcm23-281780.pdf

ECPAT International and Interpol 2018. 'Toward a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material' Retrieved from http://www.ecpat.org/wp-content/uploads/2018/03/TOWARDS-A-GLOBAL-INDICATOR-ON-UNIDENTIFIED-VICTIMS-IN-CHILD-SEXUAL-EXPLOITATION-MATERIAL-Summary-Report.pdf

Europol 2018. 'Internet Organised Crime Threat Assessment' Retrieved from https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018

Finkelhor, D 2009. 'The prevention of childhood sexual abuse', The Future of Children, vol. 19(2), pp. 169-194.

Five Country Ministerial Statement on Countering the Illicit Use of Online Spaces, 2018. Retrieved from https://www.homeaffairs.gov.au/about/national-security/five-country-ministerial-2018/countering-illicit-use-online-spaces

Floridi, L 2018. 'Soft Ethics and the Governance of the Digital'. Philosophy & Technology, vol. 31 (1), pp. 1-8.

Hamilton-Giachritsis, C., Hanson, E., Whittle, H., Beech, A., 2017. 'Everyone deserves to be happy: A mixed methods study exploring how online and offline child sexual abuse impact young people and how professionals respond to it.' Retrieved from https://learning.nspcc.org.uk/media/1123/impact-online-offline-child-sexual-abuse.pdf

House of Commons Library 2017. 'Briefing Paper. Number 06152, 28 December 2017: Business statistics'. Retrieved from https://researchbriefings.files.parliament.uk/documents/SN06152/SN06152.pdf

International Association of Internet Hotlines INHOPE 2017. 'Annual Report 2017'. Retrieved from http://www.inhope.org/Libraries/Annual_reports/INHOPE_Annual_Report_2017.sflb.ashx

Internet Watch Foundation, 2017. 'Annual Report 2017'. Retrieved from https://www.iwf.org.uk/report/2017-annual-report

Internet Watch Foundation 2018. 'Trends in Online Child Sexual Exploitation: Examining the Distribution of Captures of Live-streamed Child Sexual Abuse'. Retrieved from https://www.iwf.org.uk/sites/default/files/inline-files/Distribution%20of%20Captures%20of%20Live-streamed%20Child%20Sexual%20Abuse%20FINAL.pdf

Kloess JA, Woodhams J, Whittle H, Grant T, Hamilton-Giachritsis CE 2017. 'The Challenges of Identifying and Classifying Child Sexual Abuse Material. Retrieved from https://www.ncbi.nlm.nih.gov/pubmed/28863730

Loewenstein G and Lerner JS 2003. 'The role of affect in decision making'. In Davidson RJ, Scherer KR, Goldsmith HH. (Eds.), Handbook of affective sciences pp. 619-642. Oxford, UK: Oxford University Press

Lorenzo-Dus N, Izura C, Perez-Tattam R 2016. 'Understanding grooming discourse in computer-mediated environments'. Discourse, Context & Media, vol. 12, pp. 40-50.

Lorenzo-Dus N, Izura C 2017. '"cause ur special": Understanding trust and complimenting behaviour in online grooming discourse'. Journal of Pragmatics, vol 112, p. 68-82.

Mayer F, Arent T, Geserick G, Grundmann C, Lockemann U, Riepert T, Ritz-Timme S 2014. 'Age estimation based on pictures and videos presumably showing child or youth pornography'. International Journal of Legal Medicine, vol. 128, pp. 649-652

NetClean 2017. 'Eight Important Insights into Child Sexual Abuse Crimes'. Retrieved from https://www.netclean.com/netclean-report-2017/

NSPCC snapshot 1 2018 Children sending and receiving sexual messages. Retrieved from https://www.nspcc.org.uk/globalassets/documents/online-safety/children-sending-receiving-sexual-messages.pdf

Smith S 2012. 'Study of Self-Generated Sexually Explicit Images & Videos Featuring Young People Online'. Retrieved from https://www.iwf.org.uk/sites/default/files/inline-files/IWF_study_self_generated_content_online_011112.pdf

The Technology Coalition 2015. ' Employee resilience guidebook for handling child sexual abuse images'. Retrieved from http://www.technologycoalition.org/wp-content/uploads/2015/01/

Child Dignity
in the Digital World