PROJECT KARMA
www.projectkarma.org.au

19 August 2021

To: Parliamentary Joint Committee on Law Enforcement
Dr Sean Turner, Committee Secretary

Thank you for the invitation to make a submission to the enquiry of law enforcement capabilities in relationship to child exploitation. The following submission addresses all terms of reference.

I am the founder and Chief Executive officer of Project Karma, a Melbourne based charity focused on combatting child sexual exploitation through investigation, education and awareness, rescue and rehabilitation, and advocacy and consultation. Project Karma work in Australia and key areas of Southeast Asia.

I have been involved in the field of investigation and the prevention of child sex offences for 20 years in a law enforcement capacity with Victoria Police and as a licensed private investigator, founder of a global charity and advisor to government agencies, mainstream media, social media platform companies and associated non-government organisations in Australia and overseas.

I have found there to be very clear links across all the terms of reference, namely the need for improved collaboration, working relationships and information sharing across key stakeholders (government and non-government). These include state/territory/federal government legislations and law enforcement, non-government organisations and charities, technology providers, tourism, and behavior/psychology fields.

Other key points raised in our submission include:

- Positive developments observed across the child exploitation landscape over the last 7 years
- The important role of the WeProtect Alliance in legal communication and relationships between law enforcement and technology providers.
- The role of 'tourism' (e.g., low-cost flights, hotels), increased English language acquisition and increased internet access in more vulnerable regions, where children are more likely to be victims of online exploitation.

- The need for mirrored approaches and legislation across Australian state/territory and federal governments.
- Increased research and involvement of the medical fraternity with respect to different psychology and behaviors of offenders and preventative strategies.
- Better advocacy, understanding and preventative support for those who may be susceptible to performing a child sex offence, and/or those with Paedophilic Disorder.

We trust the Parliamentary Joint Committee on Law Enforcement will give due consideration to this submission with respect to the terms of reference.

To discuss any of the information raised please do not hesitate to contact me.

With thanks,

Glen Hulley
Founder/CEO
Project Karma
[redacted]

Inquiry into law enforcement capabilities in relation to child exploitation
Project Karma - Responses to terms of reference

A: trends and changes in relation to the crime of online child exploitation.

In commenting on the trends and changes in relation to the crime of online child exploitation it is important to understand the history and background of Project Karma (PK) and its founder/CEO Glen Hulley to provide context credentials and qualifications of the following statements.

PK (founded 2015 by Glen Hulley) is registered with the Australian Charities and Not-for-profits Commission (2016) and listed on the Australian Government Register of Harm Prevention Charities - Deductible Gift Register (2018). PK is also registered in Bali as a charitable foundation (Yayasan PK Indonesia) under the Ministry of Law and Human Rights, and Department of Social Services (2018).

Prior to forming PK Glen Hulley [1] spent 13 years in the Victorian Police force in both uniformed and covert capacities. His interest and dedication to combatting child sexual exploitation (CSE) was sparked following an experience in Cambodia where he was offered a child for sexual services. Glen has since worked with other non-government organisation's (NGO's) over 6 different counties. At one time Hulley oversaw 10 investigation teams across Southeast Asia (SE Asia). He started his own charity PK and developed an innovative and sustainability-based model for action known as 'the Sentinel Model' [2]. This model involves 3 pillars of action including 1. Community Awareness and Education, 2 Investigation, and 3 Rescue and Rehabilitation, with local ownership a key priority. In addition, PK is also heavily involved in advocacy and consultation with public, corporate and government stakeholders in Australian and overseas.

PK is an official Trust and Safety partner for Facebook (FB) including FB, Messenger, WhatsApp and Instagram). This role involves relevant monitoring and reporting to their dedicated portal with alerts and information being raised with FB and relative global law enforcement. PK also has strong relationships and consults with other online platforms such as TikTok and Roblox and Discord around protection of children against sexual exploitation.

Where Hulley and PK are only able to provide in person connection to CSE specifically over the last 7 years, the following comments are made with respects to trends and changes of online CSE over that time. With respect to the context with the above credentials and experience PK has observed and would like to comment on the following gaps and issues:

1. NGO's and charities, focused on the same or similar purposes are in competition with each other for donations and support. Whilst they ultimately fight the same battle this can create competitiveness and disjointed relationships between them, result in poor communication, lack of collaborative relationships and critical information sharing.
2. Such organisations receive critical information around these crimes, which may be fundamental to law enforcement agencies in investigating and prosecuting perpetrators. However, were relationships and partnering agreements are not in place this fundamental information can be roadblocked and delayed in reaching the required law enforcement personnel or not reach them at all. If this critical information does not reach in a timely

manner or cannot be shared with relevant law enforcement more freely the perpetrators are often long gone, or the number of children effected by the abuse is higher.

3. An example of the above points can be seen in PKs involvement in the Philippines (2016) where they (PK) and the International Justice Mission were surveying and working on the same case. As information was not shared, and there was no knowledge or discussion between to the two stakeholders, critical delays of action resulted, and precious resources being duplicated and wasted from both parties.

There are clear improvements regarding NGO's and government agencies over the last 7 years, which must be given credit for the improvements over this period. However, whilst there is improvement, there is still much to do. These crimes are still occurring, the market for these crimes is still there and relevant crimes have increased significantly, this is not a secret.

Communication and co-ordination between NGO's, law enforcement agencies, international borders and jurisdictions, government networks are lacking and disjointed. This results in less effective 'on the ground' investigations and prosecutions. PK recommend improved strategies for sharing of information and intelligence across such stakeholders in order to achieve better outcomes.

In addition, the level of involvement of social media platforms and internet companies such as Google and Microsoft also fall into this category. Where previously they have not been active, and their concerns lay in profits, there have been some major changes meaning they brought social responsibility and safety into the game. Whether it be for the safety of the community or business risk management decisions with growing government pressure, these changes have somewhat improved with significant investment on part of these companies into the safety of children. These include the need for safety and response departments and teams, around the world to review and act on reports received about potential threats of these crimes being facilitated by their platforms. The history of FB is a key example which provided a major platform for these crimes particularly between around 2011-2014. They have since developed and implemented protection departments and strategies [3, 4].

Unfortunately, COVID-19 has also introduced an additional obstacle, where such teams, due to lockdowns are having to work from home and do not have the resources normally available at the workplace. This may result in slower working processes across all major social media and gaming platforms, and thus may reflect their capacity to protect children relative to online exploitation.

B: reviewing the efficacy of and any gaps in the legislative tools and tactics of law enforcement used to investigate and prosecute offenders

Positive changes and improvements have been observed relative to legislative tools and law enforcement tactics relative to investigations and prosecution of child sex offenders. Notably the significant Australian Government investment into establishing the Australian Center to Counter Child Exploitation (ACCCE), and Daniels Law.

However, there is still significant gaps particularly in collaboration and mutual sharing of information among key law enforcement and non-government national and international stakeholders, which impact the efficiency and outcomes of actions taken by respective parties.

In Hulley's experience within Australia in particular, the legislative red-tape restrictions around obtaining information for investigations from government-based sources has led to lengthy detrimental delays in our ability to take critical action. One example of this is the 'triage' reporting system with the ACCCE, where non-government stakeholders such as PK can only communicate with the ACCCE via a public reporting portal. This creates major limitations and inefficiencies, particularly where information is highly involved, complex and/or urgent. A perpetrator may be here today and gone tomorrow, and such hurdles can create opportunities for a perpetrator to disappear. More direct communication channels and better collaboration, working relationships, contact and reporting with the Australian Federal Police (AFP) and ACCCE and may assist greatly in reducing these hurdles and the hinderance to time dependent investigations that lead to prosecutions.

It is disappointing to note that PK have developed stronger more efficient working relationships with law enforcement agencies overseas and are able to directly communicate with foreign government offices and departments immediately more effectively than they can in Australia. Where PK has proven itself time and again as an experienced, knowledgeable, and highly qualified partner in the fight against CSE, it is disheartening that the Australian government and legislation have restricted our capacity for increased contribution to the same fight of protecting children.

It is understood and appreciated that communication channel between Australian government law enforcement and non-government parties is and should be subject to very strict legal regulations around information sharing and privacy. These legislations serve to protect also. However, there needs to be some considered allowance and/or contingency, especially where it becomes a matter of immediate time-dependent and productive outcomes relative to investigation and prosecution.

One example of how these limited communication channels can affect investigation and prosecution of CSO can be seen in the case of Peter Dundas Walbran [5] of which PK was heavily involved in. Walbran was initially incarcerated for 2+ years in Lombok, Indonesia (2012) for CSE crimes. Upon release he was deported to his 'home' country Australia in 2014, where he was summoned to attend a hearing around his crimes and if appropriate placed on the CSO register. He did not attend. Instead, he sought a New Zealand (NZ) passport (as appropriate to his birth certificate) and travelled to Thailand, where PK with other authorities found him teaching in schools and abusing children. Information around his passport was not, and according to Australian legislation, could not be released to PK or other key stakeholders. It took external sources to establish this key information. Again, this was a disappointing outcome where the Australian Government may have contributed to faster and more effective results.

Due to lack of communication, information sharing, and legislation details of Walbran's place of birth, nationality and passport was not available until it was too late, delaying investigation and prosecution. As a NZ citizen, and according to NZ law (aside from COVID restrictions) he is free to travel. Where Australian has a legislative travel ban for CSO, NZ does not. Had established and direct communication and reporting channels between government and proven, valuable non-government stakeholders had been established, this may not have occurred.

From our perspective, a major gap, affecting the efficacy of legislative tools and tactics of law enforcement used to investigate and prosecute offenders is the lack of working relationships and direct communication channels between key government and non-government stakeholders.

We highly recommend that the Australian government address legislation that restricts working relationships and information sharing between proven ethical and valuable non-government parties and government law enforcement agencies, and in turn tactics of law enforcement. Attention and improvements in this area may enhance collaboration and working relationships and result in more effective time-efficient investigation and better prosecution of CSO's.

C: considering opportunities and suitability of streamlining legislative constraints to enable faster investigations that can better respond to rapidly evolving trends in offending.

PK strongly believe that better streamlining legislative constraints across Australian federal and state/territory governments would results in improved capacity to respond to rapidly evolving trends in offending and contribute to better outcomes in the future.

As outlined in the previous points, there are significant gaps in reporting platforms, collaboration and information sharing between key stakeholders including government and non-government relevant parties. These limitations to working relationships are largely impacted by restrictions imposed by current legislation. Further to the previous points, PK believe a more unified approach between state and federal governments would result in more effective working processes and outcomes, including improved control and management, and time efficient investigations.

Where state and territory legislations are not unified in their approach, there are increased opportunities for offenders to elude investigations and prosecution and commit further offences across Australian states and territories. Internet and GPS monitoring legislation for example is defined independently between states and territories. If states and territories had a more collaborative approach and mirrored a national legislation, an offender would be subject to the same repercussions no matter where they were in Australia, which may deter their movement. PK advocate for a '2 strikes out your out' policy for mandatory sentencing of CSO. If such a policy was mirrored nationally an offender would have less room to incentive to move and avoid being caught.

As a society and a government, if Australia cannot collaborate and agree on set of rules that govern how to deal with CSO in the community, there is something majorly wrong. Following this notion, PK strongly advise that a joint statement across federal and state/territory governments is needed. Should state and federal governments develop better collaborative legislation this would certainly provide evasion barriers for offenders and enhance the capacity of those such as the AFP and ACCCE.

D: considering the use by offenders of encryption, encryption devices and anonymising technologies, and Remote Access Trojans to facilitate their criminality, along with the resources of law enforcement to address their use.

Whilst PK have limited credentials in this area, they do support current international perspectives around the need for safer encryption technologies, and the dangers of end-to-end encryption with respect to CSE, restricting law enforcement from gaining critical information of offenders acting online [6, 7].

PK echo and strongly recommend the Australian government observe and consider the following statements with respect to encryption and child safety from The WeProtect Global Alliance (WPGA). This organisation works to 'transform the global response to child sexual exploitation and abuse online' as a coalition of 98 counties, including Australia [8].

> *'In light of these threats, there is increasing consensus across governments and international institutions that action must be taken: while encryption is vital and privacy and cyber security must be protected, that should not come at the expense of wholly precluding law enforcement, and the tech industry itself, from being able to act against the most serious illegal content and activity online.'*
>
> *'The WPGA, National Center for Missing and Exploited Children (US) and a coalition of more than 100 child protection organisations and experts from around the world have all called for action to ensure that measures to increase privacy – including end-to-end encryption – should not come at the expense of children's safety'* [7].

PK can vouch from experience that different online platforms facilitate grooming and child exploitation, this is also supported by research [9-11]. Where there are restrictions around the information that can be sourced by and from these online platforms by respective law enforcement agencies, the capacity to investigate and prosecute offenders is hindered. This being said, it is also fully appreciated that encryption safety measures to protect the privacy and online security of the community is also paramount.

Access to a device or screen shot of social media messages from a general encrypted platform (e.g., WhatsApp) may be sufficient to commence an investigation, however needed information such as the IP address or the tower that information came from can only be sourced from the actual company holding the server. When that companies' hands are legally tied' from releasing such information, even to legitimate law enforcement agencies, they become part of the problem.

> *'Publicly-accessible social media and communications platforms remain the most common methods for meeting and grooming children online'* [7].

For the general public, information, research and discussion around encryption may not appear relevant with views made based on blanket statements released. Where many assume their personal information is protected by encryption, it is currently not so. Many are likely unaware of current FB status or potential developments to make Messenger encrypted. Where FB are currently increasing Messenger encryption [12], there is likely less understanding from the general community around the consequences this action may mean for criminal activity.

> '*In 2018, Facebook Mesenger was responsible for nearly 12 million of the 18.4 million worldwide reports of child sexual abuse material to the US National Center for Missing and Exploited Children'* [7].

CSO's who depend on these platforms to commit their offences and run their criminal businesses however will be paying careful attention. Currently encrypted platforms cannot legally provide information to law enforcement around their activities. Those platforms where messages and information disappear immediately provide an even more disturbing opportunity for offenders to eradicate potential critical evidence.

Supporting the emerging theme of PK's submission, is the need for further communication, information sharing and stronger working relationships across key stakeholders, including technology companies are vital.

E: considering the role technology providers have in assisting law enforcement agencies to combat child exploitation, including but not limited to the policies of social media providers and the classification of material on streaming services.

Many of the concerns around this issue link with and are raised in the previous point. Technology providers as a whole have made significant progress over recent years. PK acknowledge these developments and encourage providers to continue their work in the area of combatting child exploitation within their platforms. The introduction of new features on key social media platforms are now subject to review and recommendations from their own Trust and Safety Divisions. Results from these child safety and exploitation online initiatives speak for themselves. When PK first began working in this area, Safety and Trust Divisions of social media platforms for example were not actively present and there was not the consultation there is today around child safety prior to implementing new services or initiatives [3, 7]. PK believe, if emulated and built upon internationally the positive effects of these and other recent initiatives could be even greater.

The market for online CSE will sadly always be present. There will always be those with sexual tendencies towards children, children in vulnerable positions, and those willing to exploit both factors for personal and/or business gain. Whilst it can never be stopped, strategies can be put in place to massively regress these criminal activities and reduce this horrific industry.

Whilst PK has observed positive changes over recent years, it feels confident the continuance of such developments and action is critical in order to result in a better safer landscape in the future.

It is critical that government and public pressure continue to enforce the protection of children as a primary responsibility of technology providers. These companies must continue to prioritise their resources and invest in combatting these crimes as a key component of their development and delivery of services. As technology advancement continues, so does that of perpetrators. Where the operation and profitability of such businesses are subject to strict legal obligations, these priorities will continue to be given due consideration.

Again, PK refer the WPGA [8] as a key resource for strengthening relevant policies and strategies and developing industry accountability from both legislative government and technology providers. Should technology providers establish a unified clear set of standards and guidelines, it would remove the unnecessary use of valuable resources and competitive expenditure that may be more effectively invested from both a business and social responsibility sense.

Technology provider companies have a massive influence and better collaboration and working relationships with law-enforcement and other key stakeholder is needed.

It is often in the best interests of technology providers to remove particular information off their servers as quickly as possible such as that around child exploitation material to avoid significant fines, business license restrictions and/or removal and industry embarrassment. From a business perspective significant prompt removal of such information from their servers also alleviates these businesses from accountability, risk, and responsibility. However, these are subject to rules and standards as defined by technology providers, such as those by FB, TikTok and Twitter [13-15] as accepted and agreed by users, versus legal obligations set up with law enforcement teams.

This identifies another gap between distinction of the two and potential underreporting. What information is reported to one and not the other? Again, mutual rules, international standards and ideally a recognised international body around this would assist in accountability across technology companies. However, PK acknowledges such ideologies are difficult to put in place.

The potential capacity for technology providers to assist law enforcement is huge. The better their administration and departments in these areas become, the better their assistance to law enforcement and relevant government departments investigating and prosecuting these types of crime can become. This is a very prominent area where legislation may enhance the capacity of fighting child exploitation crimes with collaborative efforts between government law enforcement and private technology provision.

F: considering the link between accessing online child abuse material and contact offending, and the current state of research into and understanding of that link.

The links between online access to child abuse material and contact offending are more pertinent to the exploitation of children overseas relative to Australian children, however Australian offenders are important clientele in this criminal industry market—This is largely due to Australia having stronger more law enforcement, more dedicated resources and less vulnerable populations compared to counties in Southeast (SE) Asia for example, where exploitation of children is easier.

An Australian offender may access live streaming or video of a child being sexually abused from such a region, do some research to find out where the information came from and attain information on how to access the information source and a particular child. PK have experienced this in their investigation firsthand. Prior to the recent COVID travel restrictions it was not difficult or relatively for such an offender to fly to a particular location and organise direct contact with a child/children for the purposes of sexual exploitation. Whilst COVID may limit current international travel, and thus such occurrences, it is only a matter of time before border re-open and direct contact offending such as this resumes. This temporary obstacle provides a time-urgent window for increased action by the Australian government to address these issues.

The concept of what is known as 'Child Rape Holidays' is not a secret. The passed legislation to ban international travel by Australian Registered Child Sex Offenders (RCSO), implemented by Senator Derryn Hinch and the Justice Party in 2017 [16, 17] of which PK was a key consultant, displays the highest level of acknowledgement of this issues and active support by the Australian Government.

With respect to links between access to online child abuse material and contact offending PK have observed serval key factors that contribute to this criminal behavior and subsequent growth over the last 5 years. These include increased English language acquisition in foreign countries, increased mobile internet data coverage access at decreased costs, budget airlines increasing foreign child access affordability; and lack of relevant education/and or training to key stakeholders on the ground (such as hotels).

Where there are higher rates of English language skills in foreign countries, there is improved communication capacity and services among the child exploitation industries and their international target markets. Increased mobile internet data and lower costs in Australia and in foreign countries also contributes to better service and access provision between CE providers (online and in person) and offenders.

Budget airlines offer very cost-effective opportunities for direct access and contact with children in vulnerable locations such as those in SE Asia. It is not unusual for travel costs between Australia and SE Asia to cost less than travel within Australia itself. Further, in such country's other costs such as accommodation, transport and food are incredibly inexpensive, making the investment of a 'child rape holiday' more financially viable to those offenders in Australia who do not necessarily have significant resources, and have not be a RCSO but are committing these crimes uncaught.

Knowledge and/or training around these crimes in key contact locations (such as international hotels) is also a variable that must be considered. To their credit there are several larger hotels and accommodation business that do provide specific workplace training and recognition and action skills to their staff around CSE and trafficking. The We Protect Children in Travel and Tourism' is an important provider of these educational and training services [18] and is another key stakeholder in the international fight against CSE in this realm.

Smaller less resourced businesses do not share the same affordability's. Where child victims are taken to, for the purpose of sexual exploitation by international 'visiting' offenders, and the capacity of that venue to recognise and act, may influence the outcome of the potentially criminal incident, and whether a child is or is not physically harmed by an Australian, or other offender.

Non-government organisations (NGO's) such as Core, the WPGA and PK itself are key stakeholders in combatting child exploitation relevant to offences in Australia and by Australian.

To reiterate, stronger communication, information sharing channels and working relationships across Australian Law Enforcement, relevant NGO's and groups, and technology providers may well result in better and faster outcomes, and less capacity for future offences to be committed.

An additional area for comment is the need for further investment and collaboration with the medical fraternity, including psychological and psychiatry around the progressive behavioral link between accessing online abuse material to physical contact offending.

PK are again not qualified in this area beyond making comment based on observations from their experiences in this field which is that this behavioral link is an unfortunate but obvious and complex one.

The patterns driving offender behaviors can differ greatly [19]. Some may not fall within the legal definition of a 'paedophile' (i.e., with some level of Paedophilic Disorder - PD) which ranges across varying thoughts, behaviors, and activities [20]. Those performing online (or otherwise) CSO may have no prior convictions and have never touched a child before, or even thought about it until an opportunity arises. This does not make them a 'paedophile'. Others will have a long a history of these characteristics. There is a lack of knowledge in community at every level, [19] around this disorder. In order to make better safer futures for children, we need to better understand the offenders of these crimes. Only then can we create effective policies and procedures that provide stronger prevention and protection.

The more that is known about the perpetrators from a medical psychiatric perspective the more governments, NGO's and law enforcement will be able to tailor their resources to prevention of contact abuse. Those with appropriate expertise in behavior and PD are in a far stronger position to identify key variables in this progression and contribute to preventative strategies. Whilst there have been commendable developments and research in this area PK believe they (the medical fraternity) need a bigger seat at the table in the development of Australian government and law enforcement strategies that aim to understand and disrupt the psychosocial factors of this link. The Australian government must further engage this medical sector and again, build stronger communication channels and collaborative working relationships with this industry in order to build more powerful and effective strategies.

Fears in society around diagnosed 'psychological' conditions and the risk of criminal repercussions may present barriers. However better knowledge and understanding around these areas, particularly from a preventative perspective, may assist in slowing the growth of the CSE industry.

G: any related matters.

In addition to the above points PK would like to add the following views in relations to law enforcement capabilities in relation to child exploitation.

1. The Australian Government needs to support better training and resources in other countries, especially where it is Australian offenders exploiting their children. PK request increased funding and investment by the Australian Government to the AFP internationally in relation to these crimes. PK focus their work and activities where they can use their limited resources to create the most impact, which as close international neighbors, is SE Asia. The Australian government should possibly consider the same principle of investing their resources where the largest impact can be made, where 'impact' is defined by number of children subjected to sexual exploitation by Australians.
2. Ad-hoc 'hit and miss initiatives do not result in long term change. Shorter term law enforcement training programs are not effective where police are transient and rotate every two to three years. A permanent presence and increased investment by the Australian Government, dedicated to child sex exploitation divisions in higher risk countries is needed.
3. Advocacy of why Australia is and should further invest in these crimes overseas – because Australians are committing these crimes against their children. We as Australians have many ex-patriots residing in these countries and many transient Australian citizen visiting. Increased law enforcement capacity in other relevant counties may not result in protecting Australian children,

but it will result in protecting children elsewhere from Australian offenders who may evade prosecution where there are gaps between key international stakeholders and communication. Surely it is our responsibility to implement as many measures as possible to protect children from exploitation by Australian citizens.

4. Where Australian offenders are prosecuted overseas, and subjected to sentence times in those countries, they may be less likely to re-offend.
5. PD (as listed in the Diagnostic and Statistical Manual of Mental Disorders) is a diagnosable psychiatric condition that cannot be 'cured' through rehabilitation or sentencing. It can only be managed with medication, therapy etc. [20]. Despite the obvious links it is important to note that those with PD and CSO's are two different things. One may or may not have harmed a child online or otherwise (but suffers from a psychiatric disorder) and the other has (by committing an offence). In Australia there is little acknowledgement or support for those with PD, online or otherwise, that have not harmed a child in any way, to manage this disorder or prevent them from progressing to a CSO. PK feel strongly that the Australian Government need to address this distinction/gap in their strategic planning and action against child exploitation.

References

1. Project Karma. *our team*. n.d.; available from: https://projectkarma.org.au/our-team/
2. Project Karma. *what we do - the sentinel project model*. n.d.; available from: https://projectkarma.org.au/what-we-do/
3. Facebook.*safety@Facebook*. n.d.; available from: https://www.facebook.com/safety
4. Facebook. *child sexual exploitation, abuse and nudity*. n.d.; available from: https://www.facebook.com/communitystandards/recentupdates/child_nudity_sexual_exploitation/
5. Murdoch, L. *convicted child abuser Peter Dundas Walbran arrested teaching at Thai school*. Sydney Morning Herald, 2015
6. Jay, J. *five eyes countries call upon tech giants to enable encryption backdoors*. 2020; available from: https://www.teiss.co.uk/five-eyes-encryption-backdoors/
7. The United States Department of Justice. *international statement: end-to-end encryption and public safety*. 2020; available from: https:www.justice.gov/opa/pr/international-statement-end-end-encryption-and-public-safety

8. WeProtect Global Alliance. *the alliance*. n.d.; available from: https://www.weprotect.org/alliance/

9. Greene-Colozzi, E.A., et al., *experiences and perceptions of online sexual solicitation and grooming of minors: a retrospective report.* Journal of child sexual abuse, 2020. 29(7): p. 836-854.

10. Quayle, E.,p*Prevention, disruption and deterrence of online child sexual exploitation and abuse.* ERA Forum, 2020. 21(3): p. 429-447.

11. Katz, C., et al., *"stop waking the dead": internet child sexual abuse and perspectives on its disclosure.* Journal of Interpersonal Violence, 2018. 36(9-10): p. NP5084-NP5104.

12. Facebook. *messenger updates end-to-end encrypted chats with new features*. 2021; available from: https://messengernews.fb.com/2021/08/13/messenger-updates-end-to-end-encrypted-chats-with-new-features/.

13. Facebook. *community standards*. n.d; available from: https://www.facebook.com/communitystandards/

14. TikTok. *community guidelines*. n.d.; available from: https://www.tiktok.com/community-guidelines?lang=en.

15. Twitter. *the twitter rules*. n.d.; available from: https://help.twitter.com/en/rules-and-policies/twitter-rules.

16. Saunokonoko, M., *'one of the most disturbing coffee breaks of my life': halting 'child rape' holidays in Asia*' 9news.com.au. 2017.

17. Australian Federal Police. *travelling child sex offenders*. n.d.; available from: https://www.afp.gov.au/what-we-do/crime-types/child-protection/travelling-child-sex-offenders.

18. We Protect Children in Travel and Tourism. *what is the code?* n.d.; available from: https://thecode.org/about/.

19. Krone, T. and R.G. Smith, *trajectories in online child sexual exploitation offending in Australia.* Trends & Issues in Crime & Criminal Justice, 2017(524): p. 1-13.

20. American Psychiatric Association, *Diagnostic and statistical manual of mental disorders (DSM-5®)*. 2013: American Psychiatric Pub.

-

PROJECT KARMA
www.projectkarma.org.au

12 October 2022

To: Parliamentary Joint Committee on Law Enforcement (PJCLE)
Lyn Beverly, Committee Secretary

Thank you for the invitation to submit additional information to our initial submission to the enquiry of law enforcement capabilities in relation to child exploitation for the new PJCLE. Project Karma (PK) would like to take this opportunity to expand information around social media, specifically Facebook (the company) and its recent rebranding to Meta. This new structure incorporates owned platforms (Facebook, Messenger, Instagram and WhatsApp) under the new Meta umbrella. Key updates refer to our original submission dated 19 August 2021:

- Point A, pg.3, para 2
- Point E, pg. 9-11

PK is an official partner of the Meta Trusted Partner Program (TPP). PK's role in this partnership involves relevant monitoring and reporting to a dedicated portal with alerts and information being raised with Meta and relative global law enforcement. As mentioned in our initial submission PK also has strong relationships and consults with other online platforms such as TikTok, Roblox and Discord around protection of children against sexual exploitation.

Supplementary comments and information (October 2022)

In addition to PK's initial submission, we believe it is very relevant to the committee to raise the developments, activities, and model of Meta, with respect to online child exploitation, since our initial submission.

Since August 2021 Meta have further invested in greater staffing levels, resources and trusted networks within its Global Safety and Trust divisions and regional bases throughout the brand's platforms. Meta has also invested in strengthening its ongoing TPP with one-off grants to NGO's actively participating in the program, including PK to further their work. As per Meta's public statement regarding TPP.

> *"Civil society organisations are critical partners in helping Meta better understand the impact of our platforms and the context of the diverse communities in which we operate around the globe. We've built the trusted partner programme to foster this partnership with civil society, strengthen the social media monitoring capacity of local organisations and improve our policies, enforcement processes and products to help keep users safe on our platforms. Our network of trusted partners includes over 400 non-governmental organisations, humanitarian agencies, human rights defenders, and researchers from 113 countries around the globe. From local organisations such as Tech4Peace in Iraq and Defy Hate Now in South Sudan to international organisations such as Internews, our partners bring a wealth of knowledge and experience to help inform our content moderation efforts. Meta provides trusted partners with funding to support our shared goals of keeping harmful content off our platforms and helping to prevent risk offline.*
>
> *We partner with expert organisations that represent the voices and experiences of at-risk users around the globe and are equipped to raise questions and concerns about content on Facebook and Instagram to:*
>
> *	*Address problematic content trends and prevent harm*
>
> *	*Foster online safety and security*
>
> *	*Inform the development of effective and transparent policies*
>
> *In addition to reporting content, trusted partners provide crucial feedback on our Content Policies and enforcement to help ensure that our efforts keep users safe. Our trusted partners' subject matter and regional expertise help strengthen our policies by enabling us to consider a range of perspectives to inform our content moderation efforts. For example, we seek*

to understand harmful misinformation by consulting with trusted partners to gain insight at the local level into what conditions and in what context certain forms of misinformation may contribute to the risk of imminent violence or physical harm, escalate social tensions, trigger violence or undermine democratic processes. These consultations enable us to develop tailored policies that help keep our community safe during times of crisis

In selecting our trusted partners, we seek organisations that have experience in social media monitoring, an interest in learning about our Content Policies, demonstrate a commitment to keeping online communities safe and represent marginalised groups who are disproportionately affected by harmful content.

We are grateful for the partnerships that we have with expert civil society organisations that help us to better understand local context, trends in speech and signals of imminent harm." [1].

Meta does not publicly share statistical data on Child Sexual Exploitation Material (CSEM), cases of online grooming, nor sexual type crimes against children detected on its platforms. Meta also does not share results of prosecution and intervention stemming from such reports. They do however publish a quarterly Global Public Transparency Report to provide updates as to the steps they are taking to protect everyone (including children) online. Current information regarding Meta's proactive approaches to online safety and its incorporation of Facebook and Instagram Safety Policies can be found online [2]

In the United States, the National Centre for Missing and Exploited Children (NCMEC) received 21.7 million reports to its global cyber tip line between 2020/2021 [3] and that millions of those reports came from Meta's current safety and reporting mechanisms.

Over the last 2 years, PK has provided over 300 reports to Meta of content on its platforms that breach its Community Standards and Safety Policies [4]. Via Meta's Law Enforcement Response Teams (LERTs) many of these reports have led to law enforcement investigations in multiple countries, including Australia. Unfortunately, PK is not advised of outcomes.

PK believe the Meta TPP model should be considered by the Committee as a minimum standards model for technology providers. Further, that it should be legislated as a mandatory requirement for all social media, instant messaging and online gaming platforms legally allowed to operate in Australia and available to people under 18.

PK believe this can be achieved through consultation between the Australian government, and application providers such as Google (Google Play) and Apple (Apple App Store) if there is legislative policy behind it.

PK hope the committee recognizes the value in the Meta TPP in building further capacity into law enforcement efforts by assisting in identifying more children at harm online and identifying platform account holders of illegal content like CSEM.

It must be noted that initiatives like the TPP only work well if sufficient training, resources, funding, and legislative powers are in place to enable law enforcement Agencies to cope with the increase of reports and the proliferation of these crimes year upon year.

Likewise for State/Territory Court Systems to have the necessary legislative powers to convict and adequately sentence the offenders.

Additional References:

1. Meta. *bringing local context to our global standards*. 2022; available from: Bringing local context to our global standards | Transparency Centre (fb.com)
2. Meta. *community standards enforcement report*. 2022; available from: Community Standards Enforcement | Transparency Center (fb.com)
3. National Center for Missing and Exploited Children. *NCMEC data*. n.d.; available from: NCMEC Data (missingkids.org)
4. Meta. *policies*. n.d.; available from: Policies | Transparency Centre (fb.com)

Australian Government
Department of Infrastructure, Transport,
Regional Development and Communications

Submission

Parliamentary Joint Committee on Law Enforcement: Inquiry into law enforcement capabilities in relation to child exploitation

August 2021

Overview

The Department of Infrastructure, Transport, Regional Development and Communications (the Department) welcomes the opportunity to make a submission to the Parliamentary Joint Committee on Law Enforcement's inquiry into law enforcement capabilities in relation to child exploitation. This submission describes the role of the Communications portfolio combatting online child sexual abuse material, the powers that will be available to the eSafety Commissioner when the *Online Safety Act 2021* comes into force in early 2022 and summarises recent Australian Government announcements regarding online safety and child safety.

The Department and eSafety have complementary roles

The Department's Digital Platforms and Online Safety Branch is responsible for providing online safety policy advice to the Government. The Department works closely with the eSafety Commissioner – Australia's online safety regulator. The eSafety Commissioner, supported by her office (eSafety) is responsible for administering complaints schemes for cyber-bullying, image-based abuse, and illegal and harmful online content, and promoting online safety in Australia. This will be extended to adult cyber abuse when the new *Online Safety Act 2021* comes into force.

eSafety works to remove online child sexual abuse material

While eSafety is not a law enforcement agency, it does contribute to responding to child exploitation online. eSafety administers the Online Content Scheme under Schedule 5 and Schedule 7 of the *Broadcasting Services Act 1992*. Under this scheme, the Commissioner may investigate valid complaints about online content, and take action on material found to be prohibited or potentially prohibited. This includes child sexual abuse material.

eSafety prioritises investigations into online child sexual abuse material and works with law enforcement agencies and the International Association of Internet Hotlines (INHOPE) to remove this content from the internet wherever it is hosted. This differs from but complements the Australian Federal Police and law enforcement agencies that focus on crime prevention and awareness raising, intelligence, investigations, disruption and prosecution of criminal offences.

For material hosted in Australia, eSafety notifies relevant Australian police and issues a takedown notice directing the hosting provider to remove the content. eSafety collects and retains relevant evidence to make sure that law enforcement investigations will not be compromised before issuing a takedown notice. Hosting providers that do not comply with a takedown notice issued by the eSafety Commissioner face penalties under the Online Content Scheme.

If child sexual abuse material is hosted overseas, eSafety work with INHOPE and the Australian Federal Police. The eSafety Commissioner is the Australian member of INHOPE, a network of 46 hotlines that works as a global mechanism to rapidly remove child sexual abuse material from the internet. If child sexual abuse material is located in an INHOPE member country other than Australia, eSafety refers the content to that country's hotline so the relevant law enforcement agency is alerted. The vast majority of content referred through INHOPE is removed in less than three working days. In the small number of cases where child sexual abuse material is hosted in a non-INHOPE member country, eSafety informs the Australian Federal Police.

eSafety will have new and strengthened powers under the Online Safety Act

On 23 June 2021, the Australian Parliament passed the *Online Safety Act 2021*. The Act bolsters Australia's world-leading online safety framework by introducing new and strengthened schemes to assist Australians when things go wrong online. The new Act will commence on 23 January 2022.

The Act preserves the Online Content Scheme that was previously set out in the *Broadcasting Services Act 1992*. The eSafety Commissioner will retain powers to issue removal notices to content hosts based in Australia and there will be civil penalties for non-compliance. Widespread industry awareness of the Scheme in Australia means formal takedowns are expected to remain rare events. Child sexual abuse material would be considered Class 1 content and therefore the Act will extend the eSafety Commissioner's powers to issue removal notices to content providers, no matter where they are located. Hosting providers will be required to take all reasonable steps to ensure the removal of child sexual abuse material, where the material can be accessed by end-users in Australia, within 24 hours or such longer period as the eSafety Commissioner allows.

The Act provides the eSafety Commissioner with a new power to issue a link deletion notice to search engine providers that provide Australians with links to class 1 material, such as child sexual abuse material. The Act also allows the eSafety Commissioner to issue an app removal notice to the provider of an app distribution service, to require the provider to cease enabling end-users in Australia to download a particular app that facilitates the posting of class 1 material within 24 hours or such longer period as the Commissioner allows. Failure to comply with a requirement under a link or app removal notice attracts a civil penalty.

The Act empowers the eSafety Commissioner to seek the creation of strengthened industry codes, or to impose industry standards. The Act includes the examples of matters to be dealt with by the codes or standards, including procedures for dealing with child sexual abuse material.

The Act also introduces a set of Basic Online Safety Expectations through a ministerial legislative instrument. This will allow the eSafety Commissioner to require transparency reports from services on how they are meeting the expectations, including how they are preventing their platform from being used to access abuse material. Failure to respond to a reporting notice from the eSafety Commissioner will incur a civil penalty.

The Department supports Home Affairs-led initiatives

The Department supports Home Affairs-led initiatives to hold the digital industry more accountable for hosting child sexual abuse material online. This includes Home Affairs' work on the Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse announced by Five Eyes countries and six major digital industry companies in March 2020. The Department also supports Home Affairs' efforts to drive a coordinated and collaborative approach with the digital industry against offenders' exploitation of online platforms to commit child sexual abuse related crimes. This is part of the first phase of the National Strategy to Prevent and Respond to Child Sexual Abuse announced in the 2021-22 Budget.

The Department recognises the important work of the Australian Federal Police and other agencies in holding perpetrators of online child sexual abuse accountable for their crimes.

The Government recently agreed to boost agency capabilities

The Department notes the Government's $146 million investment made over four years in the 2021-22 Budget for the first phase of a new National Strategy to Prevent and Respond to Child Sexual Abuse (the National Strategy). This investment will bolster the capabilities of the Australian Federal Police, the Australian Transaction Reports and Analysis Centre, the Australian Institute of Criminology, the Australian Border Force, the Australian Criminal Intelligence Commission and the Department of Home Affairs (Home Affairs) to prevent and respond to child sexual abuse. Of this, eSafety was allocated $3 million of this funding to deliver programs to help parents and families prevent online harms to children.

The Government has invested significantly to improve online safety in Australia

The Government committed $29.2 million for online safety over 4 years in the 2021-22 Budget, including $3 million for eSafety's contribution to the National Strategy. This brings the Government's total commitment to keeping Australians safe online over the next four years to over $125 million. Most of this funding is for online safety education, awareness, support and investigations. This funding will allow eSafety to fulfil its existing functions, perform additional functions under the *Online Safety Act 2021* and meet the increase in demand for resources.

Australian Government

Department of Infrastructure, Transport,
Regional Development, Communications and the Arts

Submission

Parliamentary Joint Committee on Law Enforcement: Inquiry into law enforcement capabilities in relation to child exploitation

October 2022

Overview

The Department of Infrastructure, Transport, Regional Development, Communications and the Arts (the Department) welcomes the opportunity to make a further submission to the Parliamentary Joint Committee on Law Enforcement's inquiry into law enforcement capabilities in relation to child exploitation.

This submission responds to Term of Reference (g) 'any related matters' on the capability of Australia's law enforcement agencies to tackle the growing scourge of child exploitation. It supersedes the Department's earlier submission provided in August 2021, reflecting the passage of the *Online Safety Act 2021* (the Act), which came into effect on 23 January 2022. The Act provides new and strengthened powers to the eSafety Commissioner to remove and respond to child sexual abuse material (CSAM).

Online Safety Act 2021

The Department's Online Safety Branch is responsible for providing online safety policy advice to the Government. The Act establishes the eSafety Commissioner, Australia's online safety regulator, responsible for administering schemes under the Act. The eSafety Commissioner is responsible for promoting online safety in Australia and administering complaints schemes for adult cyber abuse, child cyber-bullying, image-based abuse, and illegal and harmful online content.

eSafety's regulatory powers and responsibilities

The eSafety Commissioner supports and complements law enforcement efforts to counter online sexual exploitation of children by regulating online content, and setting standards and expectations for digital platforms to provide safe and lawful online environments. The Act empowers the eSafety Commissioner to prevent and respond to online child sexual exploitation though:

- The Online Content Scheme
- The Online Safety (Basic Online Safety Expectations) Determination 2022
- Industry Codes.

eSafety's legislative schemes allow for the receipt and investigation of complaints about harmful online content, and empower the eSafety Commissioner to order its removal from the internet. This protects Australians from exposure to harmful online content. This role complements that of Australian policing agencies who conduct criminal investigations, detecting and punishing those involved in the exploitation of children.

Online Content Scheme

eSafety administers the Online Content Scheme under Part 9 of the Act (previously contained in Schedules 5 and 7 of the *Broadcasting Services Act 1992*).

Under the Online Content Scheme, the Commissioner may investigate complaints about online content and act on 'Class 1' material no matter where it is hosted. 'Class 1' material is material that is, or would likely be, refused classification under the National Classification Scheme. Refused classification material cannot be sold, hired, advertised or legally imported in Australia, and includes child sexual abuse material (CSAM).

Informal request

Where practicable, eSafety's preference in the first instance is to draw on established relationships with services to request the removal of content. Frequently, this speeds up the removal by avoiding the need for a formal notification or notice to be prepared and issued.

Removal notice

The eSafety Commissioner may issue a removal notice to a service provider or hosting provider based in Australia requiring the removal of CSAM within 24 hours. In these instances, eSafety notifies relevant Australian police and retains relevant evidence to make sure that law enforcement investigations will not be compromised before issuing a takedown notice. Non-compliance with a removal notice may result in a civil penalty of up to 500 penalty units. The eSafety Commissioner may also issue a removal notice to service providers hosting material outside of Australia.

Service provider notification

The eSafety Commissioner may prepare and publish a public statement ('service provider notification') about a service provider hosting class 1 material in contravention of their terms of use, and provide a copy to the service provider. There is no penalty for failure to act in relation to a service provider notification. However, eSafety will consider an online service provider's response to previous notifications when considering options to deal with material.

Link deletion notice

The eSafety Commissioner may issue a link deletion notice to search engine providers that provide Australians with links to class 1 material, including CSAM. A link deletion notice can only be issued if the Commissioner is satisfied that there were 2 or more times in the previous 12 months when end-users in Australia could access class 1 material using the link, and they have already issued a removal notice which was not complied with. A link deletion notice requires the provider to cease providing a link to class 1 material within 24 hours, or face a civil penalty of up to 500 penalty units.

App removal notices

The eSafety Commissioner may issue an app removal notice to the provider of an app distribution service, in relation to an app that facilitates posting of class 1 material including CSAM. An app removal notice can only be issued if the Commissioner is satisfied that there were 2 or more times in the previous 12 months when end-users in Australia could access class 1 material on the app, and they have already issued a removal notice which was not complied with. An app removal notice requires the provider to cease enabling end-users in Australia to download the app within 24 hours. Failure to comply with a requirement under an app removal notice attracts a civil penalty of up to 500 penalty units.

Industry codes or industry standards

The Act empowers the eSafety Commissioner to seek the creation of strengthened industry codes, or to impose industry standards. The Act includes examples of matters to be dealt with by the codes or standards, including procedures for dealing with child sexual abuse material. Industry is currently developing these industry codes.

Basic Online Safety Expectations

The Act also includes a set of Basic Online Safety Expectations through a ministerial legislative instrument, which was registered on 23 January 2022. This instrument allows the eSafety Commissioner to require transparency reports from services on how they are meeting the expectations, including how they are preventing their platform from being used to access abuse material. Failure to respond to a reporting notice from the eSafety Commissioner will also attract a civil penalty. The eSafety Commissioner has issued legal notices to a number of online service providers requiring them to provide information about their efforts to prevent child sexual abuse material on their services.

Collaborative efforts

International

INHOPE

eSafety is the Australian member of INHOPE, a global network of 50 hotlines that works to rapidly remove child sexual abuse material from the internet. Where the eSafety Commissioner is made aware of child sexual abuse material located in an INHOPE member country, eSafety refers the content to that country's hotline, alerting that country's law enforcement agency to the content for investigation.

The vast majority of content referred through INHOPE is removed in less than three working days. In the small number of cases where child sexual abuse material is hosted in a non-INHOPE member country, eSafety informs the AFP.

Voluntary Principles

The Department supports AGD's work on the Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse, announced by Five Eyes countries and six major digital industry companies in March 2020.

Domestic

National Strategy to Prevent and Respond to Child Sexual Abuse (National Strategy)

Under the first phase of the National Strategy:

- eSafety has received $3.0m in the 2021-22 Budget to deliver programs to help parents and families prevent online harms to children, including sexual abuse.
- The Department supports AGD's efforts to collaborate with the digital industry against offenders' exploitation of online platforms to commit crimes related to the sexual abuse of children.

Stakeholder engagement

The Department recognises the important work of the AFP, ABF, AUSTRAC and the ACIC to investigate and disrupt online sexual exploitation of children. The Department and eSafety participate in forums chaired by the AFP-led Australian Centre to Counter Child Exploitation (ACCCE), including the Prevention Stakeholder Forum and the Research Working Group, which seek to coordinate efforts to address child exploitation across government and the non-profit sector.

Australian Government | eSafetyCommissioner

Submission

Law enforcement capabilities in relation to child exploitation

20 August 2021

Contents

The eSafety Commissioner

The eSafety Commissioner (eSafety) is Australia's national independent regulator for online safety. Our core objective is to minimise harm to Australians online.

eSafety is the first government agency in the world dedicated specifically to online safety. We lead, coordinate, educate and advise on online safety issues and aim to empower all Australians to have safer, more positive online experiences.

When eSafety was formed in July 2015 (as the Children's eSafety Commissioner), one of the agency's main functions was administering a new regulatory scheme in relation to serious child cyberbullying. eSafety also assumed responsibility for the Online Content Scheme set out in Schedules 5 and 7 to the *Broadcasting Services Act 1992* (Cth), and previously administered by the Australian Communications and Media Authority.

Since then, eSafety's functions have broadened to include administration of a civil penalties regime in relation to image-based abuse ('IBA', sometimes referred to as 'revenge porn'), the power to issue notices to content and hosting services about abhorrent violent material, and a function related to blocking websites providing access to certain terrorist content during an online crisis event.

Beyond the protections built into our authorising legislation to provide take down of harmful content and deliver compassionate citizen service, prevention through awareness and education and initiatives to promote proactive and systemic change are fundamental elements to our successful regulatory model.

In drafting this submission, we have had regard to items (a) and (e) of the Inquiry's terms of reference, along with several related matters.

eSafety's role in relation to online child sexual exploitation material

As Australia's online content regulator, eSafety plays a unique role within the Australian response to Internet-enabled child sexual exploitation. Our approach to the issue works across several axes.

Online content reports and CSEM takedown[1]

We take public reports about online child sexual exploitation material (CSEM) and other harmful content for regulatory investigation and removal under the Online Content Scheme (explained further on page 5). Of the investigations we carry forward from these reports, 99% concern CSEM and all but a handful of these items are notified to the International Association of

[1] A note about terminology. Based on the ECPAT Terminology Guidelines (also known as the Luxembourg Guidelines), the term 'child sexual exploitation material' is a broad category of content that encompasses material that sexualises and is exploitative to the child, but that does not necessarily show the child's sexual abuse. Child sexual abuse material, which shows a sexual assault against a child, is a narrower category and can be considered a sub-set of CSEM. The eSafety Commissioner receives reports about material that is both sexually exploitative and that depicts child sexual abuse. For sake of simplicity, we shall refer to CSEM throughout this submission.

Internet Hotlines (INHOPE) network for rapid removal within the host jurisdiction.[2] This serves to alleviate harm to victims and survivors, who experience re-traumatisation as a result of the images of their abuse being circulated online. The Online Content Scheme also seeks to reduce the risk of end-users accessing or being exposed to this harmful content.

Image-based abuse reports

Through the Image-based Abuse Scheme, we provide direct assistance to victims and survivors whose intimate images or videos have been shared (or threatened to be shared) without their consent. See page 6 for more information. About 25 – 30% of all IBA reports are made by Australians under the age of 18 years. Many of these reports appear to be linked with grooming and coercive behaviours. Removal is a key part of reducing the risk of ongoing harm to the children and young people who seek help from eSafety but there are cases where referral to relevant law enforcement agencies is warranted.

Australian law enforcement agencies – memoranda of understanding

In late 2020, the eSafety Commissioner concluded a memorandum of understanding with the Australian Centre to Counter Child Exploitation (ACCCE). This is a crucial agreement for the eSafety Commissioner and establishes the Australian Federal Police (AFP) as eSafety's Commonwealth law enforcement partner. The MOU addresses how and under what circumstances eSafety will notify the ACCCE about threats to children. For example, where a matter reported to us as IBA appears to involve grooming, or where CSEM reported through the Online Content Scheme depicts an identifiable child or offender. In addition, the MOU establishes how the eSafety Commissioner works collaboratively with the ACCCE on prevention, education and communications that touch on areas of mutual concern.

In addition, we have MOUs in place with every state and territory police force. These MOUs deal with a variety of matters, including notification and referral of CSEM which concerns a specific jurisdiction. For example, if CSAM were to be hosted in New South Wales, eSafety would notify NSW Police prior to removal action. Once NSW Police was satisfied that operations or investigations would not be prejudiced by removal, eSafety would proceed with takedown. We are in discussion with several states to update and refresh these agreements in preparation for the Online Safety Act 2021 (see below).

[2] The International Association of Internet Hotlines (INHOPE) is a membership organisation consisting of 46 anti-CSEM hotlines around the world. Members include the US National Centre for Missing and Exploited Children (NCMEC), the UK's Internet Watch Foundation (IWF), and France's Point de Contact. INHOPE's vision is an Internet free from child sexual abuse material, and the association works closely with domestic, international and European law enforcement (including INTERPOL and EUROPOL) to share intelligence and contribute to victim identification efforts. INHOPE was formed in 1999, and the Australian Government has been a member (first through the Australian Broadcasting Authority, then the Australian Communications and Media Authority, now the eSafety Commissioner) since 2000. Members include industry associations, charities and public authorities (including the eSafety Commissioner and the Korean Communications Standards Commission).

Prevention and education efforts

eSafety has a legislated role as the leader and coordinator of online safety education in Australia. This requires a comprehensive approach to producing guidance that addresses a range of online risks, for a variety of audiences.

Our statutory functions include supporting and encouraging measures to improve online safety for Australians; supporting, encouraging, conducting, accrediting and evaluating educational, promotional and community awareness programs relevant to online safety for Australians; and coordinating the activities Commonwealth Departments, authorities and agencies relating to online safety for children.

eSafety's education and prevention resources are evidence-based and provide extensive advice to children, young people, parents/carers and educators about a wide variety of online safety issues. We also have specialised resources for communities that may be marginalised or at greater risk of experiencing online harm.

The eSafety website includes advice about unwanted contact and grooming, how to report online exploitation (including to the AFP), and how to manage hard-to-have conversations with children about online safety. eSafety offers webinar-based training for teachers, parents and young people, including in the current series "Dealing with online harassment and image-based abuse", for parents, and "Online boundaries: it's ok to say no" for young people. This training has reached hundreds of thousands of parents, teachers and carers in the past year.

Drawing from our substantial in-house research, and collaboration with the education and early learning sector, we know that young children are increasingly given access to digital devices. By the age of four, 94% are already online. In response, eSafety provides a range of downloadable resources including a guide to online safety for parents and carers, and a set of Early Years materials. These support teaching online safety to children under five, while encouraging parents to stay engaged with their children's online lives.

As part of eSafety's role to coordinate and lift pedagogical standards in teaching online safety, we have recently published a *Best Practice Framework for Online Safety Education,* laying the foundation for a consistent national approach to education and prevention. The Framework identifies key pillars that should be in place for effective learning, including a strengths-based and age-appropriate curriculum, online safety principles taught at every year of schooling, and a balanced approach to risk and harm.

Safety by Design

Finally, eSafety has spearheaded the global roll-out of the Safety by Design initiative. Safety by Design focuses on the ways technology companies can minimise online threats to users – especially younger users – by anticipating, detecting and eliminating online harms before they occur. Embedding safety into online products and services as core features from the very outset of product design is at the heart of the Safety by Design ethos.

Key to the initiative is a framework built around principles covering platform responsibility, user empowerment, and transparency and accountability. The principles have now been translated into a set of comprehensive tools allowing companies – from start-ups to established enterprises – to evaluate the current safety of their systems, processes and practices. The tools were developed with and for industry, highlighting industry best practice in innovations for safety.

Through Safety by Design, eSafety is seeking to lift the safety standards and practices of the technology industry to ensure greater protection of users and to minimise future threats. Safety by Design is intended to shift responsibility back to the platforms for safeguarding their users and engineering out misuse before harm occurs, rather than retrofitting fixes once the damage has been done.

Regulating online harms

There are many departments and agencies at both the Commonwealth and state/territory level that share responsibility for combatting child exploitation and abuse. Important steps have been taken in Australia to create an integrated approach to tackling this harm, including where it occurs online. These steps include the watershed recommendations made through the Royal Commission into Institutional Responses to Child Sexual Abuse, the establishment of the National Office for Child Safety, and the creation of the AFP-led ACCCE.

Australian law enforcement agencies are at the very leading edge of global efforts to combat CSEM. National Joint Anti Child Exploitation Teams and specialists attached to the ACCCE work tirelessly to rescue victims and identify offenders. Over just two national operations – Operation Molto and Operation Arkstone – police arrested scores of Australians for child exploitation and laid hundreds of charges. Most importantly, at least 18 young victims were identified and made safe.

Police are to be commended for this difficult and critical work. However, law enforcement agencies cannot be expected to shoulder the effort of combatting CSEM alone. The flood of images and videos circulating on the Internet risks creating a permanent record of the abuse experienced by survivors – putting them in danger and exposing their suffering to the world at large.

As Australia's INHOPE hotline and online safety regulator, eSafety plays a complementary role to law enforcement in relation to taking down child sexual abuse imagery, while also providing direct support to young victims and survivors of image-based abuse through a civil scheme.

Many other hotlines within the global takedown network play similar roles. Public reports are encouraged through the ability to notify online CSEM anonymously, without the risk or fear of self-incrimination through a police-led reporting portal. Along with well-trained personnel, hotlines' strong and productive relationships with law enforcement support the effective management of risk. INHOPE hotlines and sister agencies contribute media and metadata to victim identification image libraries, including INTERPOL's International Child Sexual Exploitation Database (ICSE). In addition to eSafety, major global hotlines include the UK's Internet Watch Foundation (IWF), the US National Centre for Missing and Exploited Children (NCMEC), and the Canadian Centre for Child Protection (C3P).

We recognise that eSafety is part of a cross-agency, cross-sector, and multi-jurisdictional effort – one which has grown increasingly effective over recent years. To contribute to this effort, the eSafety Commissioner exercises a variety of regulatory powers.

Online Content Scheme

Schedules 5 and 7 to the *Broadcasting Services Act 1992* (Cth) (BSA) establish the Online Content Scheme. Among other things, the Scheme provides eSafety with the power to regulate the hosting of prohibited content in Australia. Whether content is prohibited is a decision made with reference to the National Classification Scheme applicable to films. Material hosted in Australia that is classified Refused Classification (RC) or X18+ will be prohibited, while material classified R18+ will be prohibited unless it is subject to a restricted access system.

Prohibited content is subject to a takedown notice, issued by the eSafety Commissioner. Takedown notices are issued against the relevant Australian hosting service provider, and must be complied with by 6pm the following business day. Non-compliance attracts a civil penalty.

As a result of the strong civil regulatory and criminal enforcement framework in Australia, prohibited material – including CSEM – is rarely hosted here. Accordingly, since 2015, the eSafety Commissioner has issued only a single takedown notice in relation to Australian-hosted prohibited material, where R18+ material was provided via an Australian-hosted adult website. Overwhelmingly, CSEM is hosted overseas and predominantly within INHOPE member jurisdictions.

Under Schedule 5 to the BSA, the eSafety Commissioner must notify Australian law enforcement in relation to overseas-hosted 'sufficiently serious material' (such as CSEM). However, so long as there is an agreement in place with an Australian police commissioner, the eSafety Commissioner may notify such material to another person or body. Through the eSafety/ACCCE MOU, eSafety has secured agreement that CSEM hosted in a country within the INHOPE Network is notified to INHOPE, with URLs hosted in other countries reported to the AFP on a regular basis. This continues a long-standing practice agreed to with the AFP since the Australian Government joined INHOPE in 2000.

In the financial year 2020/21, eSafety notified almost 13,000 CSEM items to INHOPE for removal and law enforcement action in the host jurisdiction. Media and metadata relating to verified CSEM reports processed by INHOPE are shared with INTERPOL for inclusion in its victim identification database, ICSE.

Image-based Abuse Scheme

Part 5A of the *Enhancing Online Safety Act 199* (Cth) (EOSA) sets out a regulatory scheme for investigating and acting against complaints about the non-consensual distribution of intimate images. Section 9B of the EOSA defines an intimate image as including where the image depicts or appears to depict a person's genital or anal area (including when covered by underwear), or a person's breasts if the person identifies as female, transgender or intersex, in circumstances in which an ordinary reasonable person would reasonably expect to be afforded privacy. Material is also an intimate image if it depicts a person in certain forms of private activity (for example, in a state of undress, using the toilet or showering) in private circumstances. In cases where a person's cultural or religious background involves the wearing of certain religious attire, an image will be intimate if it shows that person without the attire in a private setting.

There will be a contravention of the EOSA when a person posts or threatens to post intimate material without consent. Under the EOSA, consent to share intimate material cannot be given by a child under the age of 18. To be captured within the IBA scheme, material must be posted on (or the threat must relate to) a social media service (such as Facebook), a relevant electronic service (including messaging services such as WhatsApp), or a designated Internet service (which includes websites) and either the perpetrator or victim (or both) must ordinarily reside in Australia.

eSafety has a number of regulatory options in relation to IBA which can be directed at either the service providing access to the material or the person responsible for posting (or threatening to post) it. In cases involving a child victim and a perpetrator who is or may be an adult, eSafety is more likely to notify the perpetrator to law enforcement than to take civil action against them. The way we respond to these cases is explained in more detail below.

The Online Safety Act 2021

A major reform to the regulation of online harms will commence in January 2022 through the *Online Safety Act 2021* (Cth) ('OSA'). The OSA is intended to create a modern, fit for purpose regulatory framework that builds on the existing legislative schemes for online safety. Relevantly the OSA:

- strengthens the existing Online Content Scheme by expanding the number of services relevant to its operation, and providing the eSafety Commissioner the power to issue removal notices against 'class 1' content (which includes CSEM) wherever that content is hosted, globally
- creates new powers for the eSafety Commissioner to direct online app stores and providers of online search services to remove apps and delete links that allow access to that material where one or more class 1 removal notices have been ignored

- introduces a set of Basic Online Safety Expectations through a ministerial legislative instrument that will allow the eSafety Commissioner to require transparency reporting on how services are keeping their users safe, including how they are preventing their platform from being used as a vehicle for CSEM
- provides for the creation of one or more industry codes or standards to promote the adoption of responsible industry processes and procedures for dealing with online content issues, including CSEM.

While the provisions that relate to IBA are substantially similar to those set out in the EOSA, the interval for a service to respond to a removal notice will be reduced from 48 to 24 hours – a feature now applicable across all the OSA schemes. In addition, the OSA creates a world-first scheme to address seriously harmful adult cyber abuse, an enhanced cyberbullying scheme for Australian children and young people, and improved information-gathering powers. eSafety has produced a fact sheet on the OSA, available here.

The problem of child sexual exploitation material

The phenomenon of producing and sharing child sexual exploitation material pre-dates the Internet. However, the pre-online trade came with significant risks to offenders, reliant as it was on distributing hard copy material either through the post or via small interpersonal networks. Processing photographs and film depicting the sexual abuse of children presented considerable risk, given the need to outsource to film processing labs. In consequence, the demand for material through this period was frequently catered to by child sexual exploitation magazines with names such as *Lolita* and *Nudist Moppets.*

With the advent of dial-up Internet, the opportunity to connect with likeminded offenders with relative ease and anonymity increased substantially. Digitised versions of CSEM imagery, often scanned from magazines, were shared on bulletin boards and via email. However, file sizes were still limited by dial-up connection speeds and shaky infrastructure.

Connection speeds and bandwidth improved through the early 2000s. Alongside this technical development, digital cameras became affordable household items. It did not take long before digital cameras were integrated into mobile phones and, later, smartphones. The Internet began to abound with images produced and shared by offenders abusing children in their care. Websites, peer-to-peer networks, imageboards and forums became common and highly accessible locations to encounter CSEM.

The scale and scope of child sexual exploitation online is staggering. Far from being a threat that exists solely on the ‘dark web’, this is all too often a crime and form of abuse that is playing out in front of us. The ‘clearweb’ (that part of the Internet that is indexed and can be reached by common browsers) remains a preferred medium for the distribution and hosting of CSEM at scale. On the clearweb, well-known top-level domains such as .com and .net are routinely abused to host CSEM, and open websites provide access to hundreds of thousands of images.

The figures speak for themselves. In 2020, our sister hotline in the UK, the IWF acted on close to 155,000 reports of child sexual abuse imagery. Almost half of these reports related to ‘self-generated’ imagery (including children recording themselves performing sexual acts) – an increase of 77% on 2019. The IWF explains that some of these images appear to have been created within the context of a romantic relationship between peers, but later shared more widely online. Other images show evidence of being created through coercive, manipulative and exploitative interactions with adults.

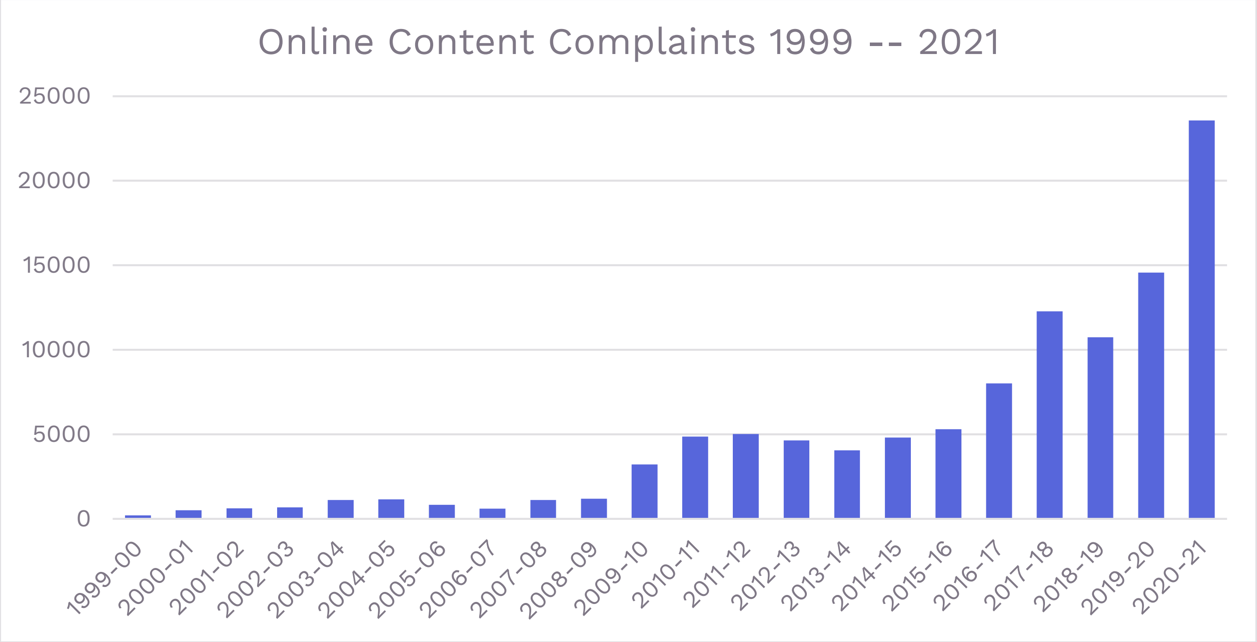
The Canadian Centre for Child Protection (C3P) has, through its Arachnid program,[3] detected and verified more than 5.4 million child sexual abuse images since 2018. Through the program, C3P has notified more than 760 electronic service providers worldwide that they are hosting CSEM. Almost 85% of the images identified through the program relate to victims that are not known to have been identified by law enforcement agencies. eSafety has partnered with C3P and contributes to the work of the Arachnid program through classification and verification of detected CSEM images, helping accelerate Arachnid's automated removal of CSEM at-scale.

During 2020, the INHOPE network exchanged reports about more than one million URLs depicting suspected CSEM. More than 90 percent of the content showed the abuse and exploitation of girls, and just over three quarters of all reported CSEM involved the abuse or exploitation of pre-pubescent children. Almost all content reported as being provided from Europe was hosted in the Netherlands.

Complaints about CSEM made to the eSafety Commissioner

Over the more than 20 years of the Online Content Scheme's operation, complaints about illegal and offensive content by the public have seen a steady increase. During the first full year of the Scheme's operation, 201 public reports were received about a variety of content types. In financial year 2020-2021, the eSafety Commissioner received more than 23,500 public reports about offensive and illegal online content. This was an increase of more than 60% on the previous financial year. Overwhelmingly, public reports concern child sexual abuse material.

[3] The Arachnid program crawls the World Wide Web for known child sexual abuse material (and related imagery) enabling automated removal notices to be sent to providers. The eSafety Commissioner participates in the Arachnid program, assisting with the classification of images identified during crawling. Arachnid is a collaboration between C3P, the Royal Canadian Mounted Police, and participating hotlines. More information can be found at https://projectarachnid.ca/en/.



Over time, eSafety has observed a distinct shift in the nature of CSEM identified through regulatory investigations, and the nature of hosting by industry. Images and videos are far more likely to have been produced by children and young people themselves, often involving explicit sexual posing and sexual touching. This type of content appears in substantial volumes on websites and forums catering to those with a sexual interest in children, and appears to often have been produced through trick, threat or manipulation.

Increasingly, CSEM websites are hosted by network providers that deliberately obscure their corporate footprint. This obfuscation can be achieved by providers registering company details in jurisdictions such as the Seychelles, distributing registration across jurisdictions, and deliberately undermining the integrity of the global WHOIS database. Some providers openly market themselves as being ‘bulletproof’: resistant to takedown and disruption and with a high tolerance to hosting illegal content. Removal of CSEM sites by INHOPE members, industry and law enforcement can be complicated by these tactics.

Classification of material on streaming services

The Australian Classification Board has worked with Netflix to create a tool allowing classification of Netflix content that is compatible with the National Classification Scheme. A 2018 review of the tool found that it produced decisions that were broadly consistent with the National Classification Scheme in 93% of cases.[4] The classification of material across delivery formats (including streaming services) will be considered by the review of Australian classification regulation currently being undertaken by the Department of Infrastructure, Transport, Regional Development and Communications.

[4] Commonwealth Department of Communications and the Arts, ‘Report on the Pilot of the Netflix Classification Tool’, <https://www.classification.gov.au/sites/default/files/2019-11/report-on-pilot-of-netflix-classification-tool_0.pdf>, 4.

eSafety has not encountered a significant problem with the classification of material on commercial streaming services such as Stan, Netflix, or Foxtel Now/Binge. During financial year 2020-21, eSafety received 2 complaints about material available on the Stan service, however the material was not deemed sufficiently serious to warrant an investigation. In the same period, we received 30 complaints about Netflix. Most of these complaints concerned *Cuties*, a film by French director Maïmouna Doucouré about an eleven-year-old Senegalese-French girl.

The film deals with various themes, in particular the hyper-sexualisation of pre-adolescent girls. While the film attracted considerable controversy for its depiction of this theme, the Australian Classification Board and Netflix tool classified the film MA15+ (Mature Accompanied). The rating's consumer advice included a warning about 'Strong themes'. Based on this rating, eSafety did not judge *Cuties* to be sufficiently serious to warrant an investigation.

Image-based abuse complaints

eSafety is the only regulator in the world to oversee a legislated civil penalties scheme for image-based abuse. Reports to eSafety about image-based abuse have also risen since the commencement of the civil penalties scheme in September 2018. About 25-30% of reports about IBA are made by those aged under 18 years. Most under-18 reporters are aged between 13 and 17 years, with only a small percentage (7%) under 13.

Of the reports received from under 18s, most concern online child sexual exploitation. Only 8% concern peer-group sharing. Young reporters are typically coerced into sharing images of themselves by adult offenders, who are often pretending to be young people. Once a young person has sent an image to this type of offender, threats to share their images are received and demands are made for further images. We have developed procedures which ensure eSafety is a safe place for children and young people to come for help with these matters. These procedures align with our obligations to provide relevant information to police, including to the ACCCE.

eSafety is strongly committed to working with police to hold offenders accountable and we regularly notify information to achieve this shared objective. We manage risks to the relevant child or young person by ensuring that they cease all contact with the offender, and we work with the relevant online platform to have the child's image and/or the offender's account removed (in consultation with the ACCCE, where relevant). Over the life of the IBA scheme, eSafety has alerted social media services to the misuse of almost 500 accounts involved in the sexual exploitation of a child or young person, with services disabling over 80% of the accounts reported. We also refer children and young people to Kids Helpline for counselling and support.

Where peer-group sharing is relevant to a report, we have found that a law enforcement approach is not always a preferable option for resolution. While these matters are typically reported to police by either school staff or parents, police for a number of reasons do not always elect to prefer charges. This decision might be due to insufficiency of evidence, or the age and vulnerabilities of the children involved. We typically address this type of matter by:

- reporting accounts that have shared, or threatened to share, intimate images to the social media service
- giving advice on how the victim can screenshot evidence (for example, of threats or account profiles) and block accounts
- providing safety advice regarding privacy settings and deleting all friends/followers who are not known and trusted offline.

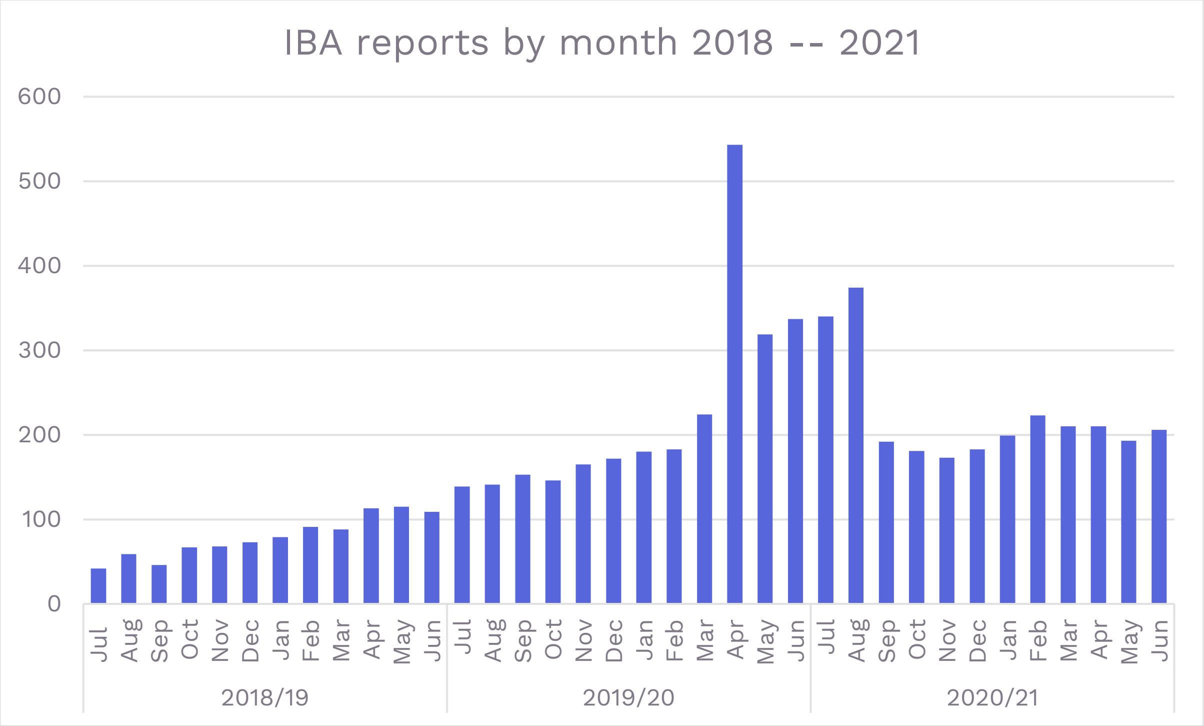
We might also:

- liaise with schools if they are in a position to help address the incident
- speak with police if they are already involved or ought to be involved

- take remedial action, for example, by writing to the young person/s responsible for the non-consensual sharing, warning them that their actions are unlawful and requiring confirmation that they have deleted the intimate images from their devices and anywhere they may have posted them online.

eSafety has received more than 6,400 reports about IBA over the life of the scheme.

Almost 70% of all reports have been received in the last 18 months alone.



eSafety's research shows that Australian teens are exposed to a range of risks and threats online. More than 40% of young Internet users report negative experiences online. These include being contacted by a stranger (30%) and receiving inappropriate or unwanted content such as pornography (20%).[5] While many teens take some form of action against the unwelcome contact, less than half mention it to family or friends (43%) or report it (40%).[6] Online safety information is valued by teens, with three-quarters wanting information about issues such as how to block bad actors, how to support friends in trouble, and how to report negative online experiences.[7]

All of this makes clear that the prevalence and accessibility of CSEM online is a challenge that goes well beyond law enforcement. Instead, addressing the many elements that enable the online sexual exploitation of children demands a whole-of-government, whole-of-community

[5] eSafety Commissioner, *The digital lives of Aussie teens*, <https://www.esafety.gov.au/sites/default/files/2021-02/The%20digital%20lives%20of%20Aussie%20teens.pdf>, 5.
[6] Ibid, 6.
[7] Ibid.

approach that reaches across borders and jurisdictional limits. The eSafety Commissioner plays an active role in this response through our regulatory interventions, education and prevention initiatives, and policy innovations such as Safety by Design.

The role of technology providers in assisting law enforcement and governments

Industry's policies overall

Most mainstream services have policies, rules, terms of use or community standards prohibiting child sexual exploitation and abuse on their platforms. When they become aware of such content, mainstream services which are subject to US federal law typically remove it, disable the relevant account, and report it to NCMEC. NCMEC forwards the reports to law enforcement agencies around the world, including the AFP. In 2020, NCMEC received 21.4 million reports from electronic service providers related to suspected child sexual exploitation shared via their networks or held in their data storage systems.[8]

Services detect and action CSEM in a variety of ways, including through Trust and Safety teams and automated tools. Some of this work is proactive, such as scanning content for potential CSEM at upload, and some is reactive, such as providing reporting mechanisms for users to notify potential CSEM to the service. As outlined below, the effectiveness of these measures varies across services, as does the level of investment, innovation and collaboration undertaken to combat CSEM.

Another variable element is the level of transparency that services provide in relation to these efforts. Many transparency reports remain centred on government requests for content removal. However, services are increasingly beginning to report on the amount of CSEM discovered on their platforms through proactive tools and user reports, in addition to the items surfaced through government notices. Reports may also set out the number of accounts disabled and items of content removed and reported to NCMEC, as well as providing details about other initiatives, projects and partnerships in this space.

There are several groups currently working to drive up industry practices and standards through collective action. These include the industry-led Technology Coalition and the cross-sector, multi-stakeholder WePROTECT Global Alliance (WPGA). The eSafety Commissioner serves as a member of the WPGA Board and recently coordinated Australia's response to the WPGA's survey on implementation of the Model National Response, a blueprint for national action to tackle online child sexual exploitation.

[8] National Centre for Missing and Exploited Children. '2020 Reports by Electronic Service Providers (ESP), <https://www.missingkids.org/content/dam/missingkids/gethelp/2020-reports-by-esp.pdf>.

eSafety's experience in working with industry on CSEM issues

Efforts by major industry representatives to harden their platforms and networks are welcomed by eSafety. Several initiatives – some longstanding – have had a tangible impact on the ability of offenders to find, share and store CSEM online.

They include:

- Google: In many countries, users who attempt to locate CSEM via Search are met with Google Ads showing deterrence messaging. In Australia, this messaging warns users that the 'intentional viewing or possession of sexually explicit imagery of minors is illegal'. A reporting link to the eSafety Commissioner is provided, along with information about contacting the AFP and assisting victims of child sexual abuse through Bravehearts. Google also provides its Content Safety API – an artificial intelligence classifier for CSEM – to customers for free. The API is intended to help organisations scale and prioritise decisions around content remove content. YouTube also freely offers its CSAI (Child Sexual Abuse Imagery) Match technology, allowing for detection and matching of known child sexual abuse video content.
- PhotoDNA: A key tool in the identification and removal of CSEM at scale is PhotoDNA. This is a 'hashing' technology able to convert images into a unique signature. This signature can be used to find similar images, and is used widely by industry and NGOs such as C3P and NCMEC to detect, notify and remove known CSEM. PhotoDNA was developed in 2009 through a partnership between Microsoft and Dartmouth College in the United States. The technology is offered free as a cloud service to qualified organisations.
- Other hashing technologies: Facebook has released two hashing algorithms as open-source projects to assist with detecting CSEM. Known as PDQ and TMK+PDQF, the algorithms allow for perceptual hashing of images and videos, respectively. Both are offered free from a public GitHub repository.
- Project Artemis: An anti-grooming tool developed by Microsoft in collaboration with The Meet Group, Roblox, Kik and Thorn. The tool is made freely available by Thorn to qualified organisations that offer a chat function as part of their service. Artemis helps with moderation of high-risk conversations on platforms that flag potential grooming efforts, and is based on technology originally deployed by Microsoft on its Xbox gaming platform.
- Apple: Recently, Apple announced its commitment to preventing its products and services from being misused to distribute CSEM. Starting with efforts to limit the potential for children to come to harm using Apple technology, the company will soon add new tools to warn children and their parents when receiving or sending messages containing nudity. In addition, on-device hashing of images will now occur in a way that preserves privacy while allowing detection of CSEM. Finally, Apple will provide warnings and information to those who attempt to search for CSEM using Apple services.

However, there are still areas that warrant improvement.

For example, in early 2021 the Canadian Centre for Child Protection (C3P) analysed the reporting functions provided to users by major platforms.[9] While most platforms provided a way for users to report illegal or inappropriate content, there were few cases where a CSEM-specific option was provided. In addition, C3P identified several features that created inhibitions against reporting, such as requiring users to provide personal contact information, requiring users to create an account before being able to flag content, and an inability to report specific users, profiles, posts or a combination.

In 2020, eSafety identified a number of accounts on a major platform that appeared to have been created for the sole purpose of sharing CSEM. The accounts were often private but displayed specific indicators that strongly suggested their purpose. For example, many referred to popular file-hosting platforms such as Mega, displayed images of known CSEM victims in their profile, and contained text such as 'DM to trade' and 'cheese pizza' (shorthand for 'child pornography'). Even though no content was posted to these accounts, they often had follower counts in the thousands. At the time, eSafety noted that there was no way to report entire accounts for CSEM-related violations.

Shortly after discussing its internal report with the ACCCE, eSafety sought a meeting with senior platform representatives. During the meeting, the eSafety Commissioner explained the key indicators we identified as suggesting that accounts were CSEM-related and explained our concerns with the sufficiency of reporting options. The company representatives undertook to review their processes and some changes were made to detection and reporting procedures. We have observed a reduction – but not an elimination – of these kinds of reports.

eSafety remains concerned at the lack of progress made within industry overall on the issue of content that is related to but does not depict CSEM. Overwhelmingly, survivors of online child sexual abuse are concerned about the potential for their abuse material to become known to those in their lives. More acutely, many survivors fear recognition by strangers from their abuse material. Sadly, this is all-too-often a fear that is justified, with 30% of survivors surveyed in a 2017 study by C3P disclosing that they had been identified online or in-person by someone who had seen their abuse imagery.[10] Survivors have been physically followed, threatened and propositioned as a result of being recognised and targeted.

While industry tends as a rule to remove clear CSEM from its networks and storage services, there is far less commitment to removing related material. The sexual abuse and exploitation of children online frequently occurs within a context of an image series showing the child dressed, and then in various states of undress prior to the depiction of contact offending (for example penetrative sexual assault). The 'scene-setting' images within a series can be just as harmful to survivors when available online, as they form part of a continuum of abuse that remains fresh and distressing. Even though they may not be illegal per-se, the images are a reminder of trauma and warrant removal.

However, it can be a challenge for hotlines and others working in content removal from a victim perspective to persuade industry that these images should be removed. Often, industry will remove material only when it is illegal within a specific jurisdiction, and in some cases efforts to

[9] Canadian Centre for Child Protection, *Reviewing Child Sexual Abuse Material Reporting Functions on Popular Platforms*, <https://protectchildren.ca/pdfs/C3P_ReviewingCSAMMaterialReporting_en.pdf>, 8.

[10] Canadian Centre for Child Protection, *Survivors' Survey Full Report,* <https://protectchildren.ca/pdfs/C3P_SurvivorsSurveyFullReport2017.pdf>, 165.

take down CSEM-related material are met with resistance. There is also reluctance to removing written accounts of adults sexually abusing children or illustrated and drawn depictions of sexual abuse (even though they are prohibited in several jurisdictions including Australia). We note that internationally a schism is forming around content that is 'illegal' and content that still extremely harmful but is legal. Proposed legislation and regulatory approaches in the UK (Online Safety Bill), Canada (Discussion guide), Ireland (Online Safety and Media Regulation Bill) and the EU (Digital Services Act) grapple with this issue, to varying degrees.

We are concerned with using illegality as the vector to determine whether industry should act in response to harmful content. With this type of approach, a huge spectrum of online harms would fall through the cracks of regulation and response, ultimately leading to individual harm. Online platforms should retain the prerogative to identify harmful content based on users' complaints for illegal and harmful content, to safeguard children and all citizens online.

It can be seen, then, that there is still much work to do. Noting this, it is worth emphasising how critical a partner industry is in counter-CSEM efforts. The modern Internet – its wires, hardware, data centres, and cabling – is almost entirely owned and operated by private concerns. That means that efforts to harden the online world against abuse by those producing and distributing CSEM will only be effective with sustained and systemic buy-in from the network operators, domain registrars, Internet address registries, domain administrators, hosting service providers, enterprise cloud providers and others. This requires sustained cross-jurisdictional efforts and consistency of regulation, globally.

Key Challenges

Encryption

Digital encryption is not new and, in its modern form, has been used for more than 40 years as an essential tool for privacy and security. It is primarily employed to keep data and transactions secure and to prevent data breaches and hacking. It allows legitimate, positive and safe communication where this may not otherwise be possible, and is used to protect valuable information such as passport credentials.

However, encryption can also assist in serious harms by hiding or enabling criminal activities, including online child sexual abuse. Technologies that detect illegal material by proactively scanning, monitoring and filtering user content currently do not work on systems that use end-to-end encryption (E2EE). Because of this, E2EE can facilitate the production, exchange and proliferation of child sexual abuse material, perpetuating the abuse of victims and exposing survivors to ongoing trauma.

A drift towards E2EE by major social media platforms will make investigations into serious online child sexual abuse and exploitation significantly more difficult. It will create digital hiding places, and platforms may claim they are absolved of responsibility for safety because they cannot act on what they cannot see.

We know there are a number of solutions that would ensure illegal activity online can be addressed. These work without compromising encryption while allowing lawful access to information needed in serious criminal investigations. Solutions include using certain types of encryption that allow proactive tools to function, implementing proactive detection tools at transmission, rather than on receipt, and moving AI and proactive technical tools to the device level (as Apple is doing).

Anonymity and identity shielding

Anonymity and identity shielding allow a user to hide or disguise their identifying information online. Anonymous communication is a cornerstone of promoting freedom of speech, expression and privacy on the Internet, but it can also be misused to control and abuse people.

Technical approaches to anonymity include software, browsers and encrypted or decentralised platforms. Examples include virtual private networks that mask the user's location and device details (IP address), anonymising processes that conceal the link between a message and the sender, and E2EE that allows only a sender and recipient to decode digital content.

Simpler approaches involve taking on a fictional identity. Examples include using a false name (i.e., a pseudonym or alias), a virtual representation (or avatar), or a fake profile.

Most investigations into CSEM involve individuals posting the content online anonymously. These investigations have shown that content contributors will go to great lengths to remain anonymous, often using one or more anonymising security measure to hide their identities.

Sexual predators also commonly use anonymous, fake, imposter and impersonator accounts to lure victims and gain their trust. For example, they may use an avatar in a game to pretend they are the same age and gender as a child so they can become a fake friend and groom them for sexual interaction.

It is very difficult for regulators and law enforcement to identify and act against individuals and using fake accounts. It also makes it almost impossible for social media services and other users to deal with abusers breaching the terms of service, through strategies such as blocking and suspension, as well as preventing, detecting and removing multiple accounts operated by one user.

A balance is needed, where the misuse of anonymity and identity shielding is restricted without removing any of the legitimate benefits. Steps can be taken by services to verify accounts before users start to operate them, or to take down accounts that violate the terms of service and prevent them from resurfacing.

Decentralisation

Decentralisation of the Internet means widely distributing the control of the online data, information, interactions and experiences of users so they are no longer reliant on a concentration of large technology companies that own or operate mainstream, centralised servers (the computer hardware and software that stores data) to access the online world.

While decentralisation can allow users to protect their information and control their online experiences, it can also make it more difficult to hold users (or the entities behind them) responsible for illegal and harmful content and conduct. The lack of a central authority, along with the storage and distribution of data across many computers, makes it difficult to moderate or regulate decentralised services and platforms or enforce the removal of illegal and harmful content. For these reasons, there are concerns that a decentralised Internet may become a haven for CSEM and for users who have been removed from mainstream services and platforms.

As interest grows in the tech community to develop the 'DWeb' and 'DApps', and as mainstream platforms increasingly respond to and address CSEM on their services, the perceived impenetrability and unaccountability of decentralised environments could act as an incentive for those with nefarious intent to evade detection, to preserve their 'collections' of materials and to further create and distribute CSEM.

We must work collectively and across borders to encourage greater consistency and shared approaches to help counter online risks and harms on decentralised services and platforms. There is also need to ensure that safety-by-design is given the same priority as security- and privacy-by-design in the design and development of decentralised services and in the broader Web 3.0 infrastructure.

There are a number of ways decentralised services and platforms can help to keep their users safe from online harms. For example, online communities can opt-in to moderation and governance arrangements. Features such as voting systems can allow users to decide acceptable conduct and accessible content. Additionally, built-in incentives, such as micropayments or other rewards, may encourage positive behaviour and safer environments. Decentralised services and platforms can also be built using technology protocols that allow third party content moderation tools to function. For example, tools that scan for child sexual abuse material might be adopted, though their operation would have to be agreed to by the community of users.

Addressing Challenges through Safety by Design

eSafety recognises that encryption, anonymity and decentralised systems may help to protect certain elements of privacy and security. Our focus is on working with industry and developers to ensure that services are aware of Safety by Design principles and adopt them, so the risks of these features are considered along with the benefits.

The initiative has been developed with industry for industry. It recognises that, if we wish to end child sexual exploitation and abuse, industry needs to be at the heart of any process to effect cultural change through enhanced corporate social responsibility. eSafety has undertaken extensive consultation with industry, civil society organisations, advocates, parents and young people themselves to understand how online harms develop and are experienced across broad and intersectional communities.

As noted above, our Safety by Design principles have now been translated into a set of comprehensive tools allowing companies – from start-ups to established enterprises – to evaluate the safety of their systems, processes and practices. This includes advising industry on how to ensure that robust moderation of conduct and content is possible before releasing products to the market, as well as how to authenticate users and prevent known techniques used by perpetrators to target and abuse others.

Safety by Design encourages technology companies, and indeed the broader technology industry, to help end child sexual exploitation and abuse by enhancing their corporate social responsibility. In part, this can be done by highlighting the innovation that is already occurring within the sector as well as encouraging technology companies to foster a global community and to be open in sharing their solutions.

User-centred design with consideration of children and young people is critical. Key touchpoints for industry consideration include implementing default privacy and safety settings at the highest possible levels, incorporating conversation controls and discoverable and seamless reporting pathways. Such measures proactively address the potential for online harm, while empowering users to regulate their own online experiences.

eSafety continues to work closely with industry to further implement existing safety measures, standards, requirements and guidance – as well as encourage them to innovate and transform the safety landscape further. Our forward workplan for Safety by Design includes working with the investment community to incorporate the principles into responsible investment practices; generating practical engagement with the assessment tools within the start-up community; focusing on marginalised and at-risk groups to ensure their needs are considered; and developing targeted resources for new and emerging sectors.

Submission

Law enforcement capabilities in relation to child exploitation

October 2022

Contents

Foreword

The eSafety Commissioner (eSafety) welcomes the continuation of the inquiry into law enforcement capabilities in relation to child exploitation.

eSafety provided a submission to the inquiry's previous consultation in August 2021. Since then, there have been several updates to our work activity in relation to child sexual exploitation material (CSEM) that may be valuable for the Committee's consideration. This submission provides updated information and data where relevant.

The eSafety Commissioner

eSafety is Australia's national independent regulator for online safety. Our core objective is to minimise harm to Australians online.

eSafety is the first regulator in the world dedicated specifically to online safety. We lead, coordinate, educate and advise on online safety issues and aim to empower all Australians to have safer, more positive online experiences.

When eSafety was formed in July 2015 (as the Children's eSafety Commissioner), one of our main functions was administering a new regulatory scheme in relation to serious child cyberbullying. eSafety also assumed responsibility for the Online Content Scheme set out in Schedules 5 and 7 to the *Broadcasting Services Act 1992* (Cth), previously administered by the Australian Communications and Media Authority (ACMA). The Online Content Scheme empowered eSafety to investigate complaints and facilitate removal of prohibited content hosted in Australia, including CSEM.

Since then, eSafety's functions have broadened to include administration of a civil penalties regime in relation to image-based abuse (sometimes referred to as 'revenge porn'), the power to issue notices to content and hosting services about abhorrent violent material, and a function related to blocking websites providing access to certain terrorist content during an online crisis event.

In January 2022, the *Online Safety Act 2021* (Cth) ('OSA') came into effect. Relevantly, the OSA introduced new powers for eSafety, including strengthening and extending eSafety's existing powers under the Online Content Scheme and providing new tools to regulate services' systems and processes. This includes enabling eSafety to require online service providers to report on the steps they are taking to comply with the Basic Online Safety Expectations, which outline the Australian government's expectations for certain types of online services to minimise material or activity that is unlawful or harmful. The Act also provides for representatives of sections of the online industry to develop new industry codes relating to the online activities of participants in those sections of the online industry. The industry codes are intended to regulate illegal and restricted content, including CSEM.

Other fundamental elements of our successful regulatory model include prevention through awareness and education and initiatives to promote proactive and systemic change.

Our Regulatory Posture and Regulatory Priorities 2021-22, published in November 2021, outlines eSafety's current focus areas. The rapid removal of CSEM continues to be one of our highest priorities.

We have also recently published our inaugural corporate plan 2022-23 to provide transparency to government and the public of eSafety's purpose, objectives and measures of success when addressing CSEM. In August 2022, we released our four-year strategy for 2022-25, which outlines how we will continue to protect Australians from exposure to child sexual exploitation.

In updating this submission, we have had regard to items (a) and (e) of the Inquiry's terms of reference, along with several related matters.

eSafety's role in relation to CSEM

As Australia's online safety regulator, eSafety plays a unique role within the Australian response to Internet-enabled child sexual exploitation. Our approach to the issue works across several axes.

Online content reports and CSEM takedown

We receive complaints from the public about CSEM[1] and other illegal or harmful online content. We are able to conduct regulatory investigations and require removal of certain material under the newly expanded Online Content Scheme (explained further on page 5). Of the investigations we carry forward from these complaints, 99% relate to CSEM and all but a handful of these items are notified to the International Association of Internet Hotlines (INHOPE) network by eSafety for rapid removal within the host jurisdiction.[2] The removal of material serves to alleviate harm to victims and survivors, who experience re-traumatisation as a result of the images of their abuse being circulated online. The Online Content Scheme also seeks to reduce the risk of end-users accessing or being exposed to illegal or harmful online content.

Image-based abuse reports

Through the Image-based Abuse Scheme, we provide direct assistance to individuals whose intimate images or videos have been shared (or threatened to be shared) without their consent. About 25-30% of all image-based abuse reports to eSafety are made by Australians under the age of 18 years. Most reports concern offenders coercing children, particularly teenage males, into producing explicit images of themselves and then extorting them.

Since our previous submission, we have strengthened our processes for referrals to the Australian Federal Police (AFP)-led Australian Centre to Counter Child Exploitation (ACCCE), the national coordination mechanism for online child sexual exploitation and abuse. The ACCCE works to investigate these crimes while eSafety delivers complementary services, such as facilitating content removal, taking certain remedial actions, and providing information about support services and online safety. eSafety also works with the ACCCE and others across government on systemic change to limit offender access to Australian children on high-risk platforms.

[1] A note about terminology: Based on the ECPAT Terminology Guidelines (also known as the Luxembourg Guidelines), the term 'child sexual exploitation material' is a broad category of content that encompasses material that sexualises and is exploitative to the child, but that does not necessarily show the child's sexual abuse. Child sexual abuse material, which shows a sexual assault against a child, is a narrower category and can be considered a sub-set of CSEM. The eSafety Commissioner receives reports about material that is both sexually exploitative and that depicts child sexual abuse. For sake of simplicity, we shall refer to CSEM throughout this submission.

[2] The International Association of Internet Hotlines (INHOPE) is a membership organisation consisting of 46 anti-CSEM hotlines around the world. Members include the US National Centre for Missing and Exploited Children (NCMEC), the UK's Internet Watch Foundation (IWF), and France's Point de Contact. INHOPE's vision is an Internet free from CSEM, and the association works closely with domestic, international, and European law enforcement (including INTERPOL and EUROPOL) to share intelligence and contribute to victim identification efforts. INHOPE was formed in 1999, and the Australian Government has been a member (first through the Australian Broadcasting Authority, then the Australian Communications and Media Authority, now the eSafety Commissioner) since 2000. Members include industry associations, charities, and public authorities (including the eSafety Commissioner and the Korean Communications Standards Commission). We may not notify investigations to INHOPE if the material is hosted in a non-INHOPE member country, and will instead refer the matter to the ACCCE.

Australian law enforcement agencies – memoranda of understanding

In late 2020, eSafety established a memorandum of understanding (MOU) with AFP. This is a crucial agreement for eSafety and establishes the AFP as eSafety's Commonwealth law enforcement partner.

The MOU addresses how and under what circumstances eSafety will notify the ACCCE about threats to children. For example, where a matter reported to us as image-based abuse appears to involve grooming, or where CSEM reported through the Online Content Scheme depicts an identifiable child or offender, that will be referred to the ACCCE regardless of jurisdiction. The ACCCE will triage the information and, if necessary, refer that to the relevant jurisdiction. In addition, the MOU establishes how eSafety works collaboratively with the ACCCE on prevention, education and communications that touch on areas of mutual concern.

With the commencement of the OSA in January 2022, the MOU with the AFP is currently being updated and will include a Letter of Exchange detailing updated information-sharing arrangements, such as content referrals and intelligence, between eSafety and the ACCCE.

In addition, we have MOUs in place with every state and territory police force, which are also being updated following the commencement of the OSA.

Prevention and education efforts

eSafety has a legislated role to improve and promote online safety for Australians, which includes supporting and encouraging online safety education in Australia. This requires a comprehensive approach to producing guidance that addresses a range of online risks, for a variety of audiences.

Our statutory functions include:

- supporting and encouraging measures to improve online safety for Australians
- supporting, encouraging, conducting, accrediting, and evaluating educational, promotional and community awareness programs relevant to online safety for Australians
- coordinating the activities of Commonwealth Departments, authorities and agencies relating to online safety for Australians, including children.

eSafety's education and prevention resources are evidence-based and provide extensive advice to children, young people, parents and carers, and educators about a wide variety of online safety issues. We also have specialised resources for communities that may be marginalised or at greater risk of experiencing online harm.

The eSafety website includes advice about unwanted contact and grooming, how to report online exploitation (including to the AFP), and how to manage hard-to-have conversations with children about online safety. eSafety offers webinar-based training for teachers, parents and carers and young people, including in the current series 'Dealing with online harassment and image-based abuse' for parents, and 'Online boundaries: it's ok to say no' for young people. This training has reached 133,936 parents, carers, and teachers during 2021-22.

Drawing from our substantial in-house research, and collaboration with the education and early learning sector, we know that young children are increasingly given access to digital devices. 94% of children in Australia are already online by the age of 4 years. In response, eSafety provides a range of downloadable resources including a guide to online safety for parents and carers, a set of Early Years materials and recently released materials for 5–8-year-olds. These resources assist both parents and teachers and encourage them to stay engaged with children's online lives.

As part of eSafety's role to coordinate and lift pedagogical standards in teaching online safety, we have published a *Best Practice Framework for Online Safety Education*, laying the foundation for a consistent national approach to education and prevention. The Framework identifies key pillars that should be in place for effective learning, including a strengths-based and age-appropriate curriculum, online safety principles taught at every year of schooling, and a balanced approach to risk and harm.

Additionally, as part of the National Strategy to Prevent and Respond to Child Sexual Abuse, eSafety is delivering the Families Capacity Building Project. The project delivers targeted education that supports vulnerable families to recognise and prevent harmful behaviours online, with a specific focus on issues related to online child sexual exploitation and child safety.

Safety by Design

Finally, eSafety has spearheaded the Safety by Design initiative. Safety by Design focuses on the ways technology companies can minimise online threats to users – especially younger users – by anticipating, detecting, and eliminating online harms before they occur. Embedding safety into online products and services as core features from the very outset of product design is fundamental to the Safety by Design ethos.

At the heart of the initiative are three principles covering platform responsibility, user empowerment, and transparency and accountability. The principles have now been translated into a set of comprehensive risk assessment tools allowing companies – from start-ups to established enterprises – to evaluate the current safety of their systems, processes, and practices. The tools were developed with and for industry, highlighting industry best practice in innovations for safety.

Our Safety by Design resources have been accessed in over 46 countries and have become a critical element of emerging policy and regulatory initiatives around the globe. We continue to work with stakeholders to enhance online safety awareness and to cement Safety by Design into policy and regulatory dialogues and as a critical element in industry best practice.

Online Content Scheme

The regulation of illegal and restricted online content, including CSEM, is provided for under the strengthened Online Content Scheme within Part 9 of the OSA.

The OSA establishes two classes of material for regulatory action: class 1 and class 2. Whether material is class 1 or class 2 is a decision made with reference to the National Classification Scheme applicable to films, publications, and computer games. Class 1 material is that which is, or is likely to be, classified Refused Classification (RC), and includes CSEM, pro-terror material, and material that instructs, incites, or promotes in matters of crime and violence. Class 2 is material that is, or is likely to be, classified either X18+ (or Category 2 restricted) or R18+ (or Category 1 restricted) and is provided from Australia.

Where material is identified as being class 1 material, the eSafety Commissioner can give a removal notice to the service providing the material (i.e. a social media service, relevant electronic service, or designated internet service) or the hosting service provider, regardless of where in the world the material is hosted. Services have 24 hours to comply with a notice, and non-compliance may attract a civil penalty.

Non-compliance with a class 1 removal notice given under the OSA enlivens additional notice powers to minimise the impact of harm caused by Australian end-users having access to the material. A link deletion notice can be given to the provider of a search engine service in certain circumstances and requires the service to stop providing a link to the material through search results. An app removal notice can be given to the provider of an app distribution service in certain circumstances and requires the service to stop allowing Australian end-users to download an application that is providing access to class 1 material.

Under Section 224 of the OSA, the eSafety Commissioner must notify Australian law enforcement in relation to 'sufficiently serious material' which includes CSEM. Based on an existing agreement with the AFP, eSafety notifies INHOPE of CSEM hosted in a country within the INHOPE Network, with URLs hosted in other countries reported to the AFP on a regular basis. This continues a long-standing practice agreed to with the AFP since the Australian Government joined INHOPE in 2000.

Where information that may lead to the identification of a victim or offender is found as part of our investigations, we provide this to the ACCCE for their consideration. The arrangements for sharing information between eSafety and the ACCCE are contained within a letter of exchange, which operationalises the provisions of the eSafety/AFP MOU.

The efficacy of the INHOPE network in facilitating the rapid removal of CSEM means that referral through the network is eSafety's preferred operating method. In 2021, almost 1 million URLs of CSEM were reported through the INHOPE network, with 79% removed within 6 days.

As a result of the strong civil regulatory and criminal enforcement framework in Australia, illegal and restricted online material, including CSEM, is rarely hosted here. Accordingly, since 2015, the eSafety Commissioner has issued only a single takedown notice in relation to Australian-hosted material under the Online Content Scheme. Overwhelmingly, CSEM is hosted overseas and predominantly in other INHOPE member jurisdictions.

In the financial year 2021/22, eSafety notified almost 11,000 CSEM items to INHOPE for removal and law enforcement action in the host jurisdiction. Media and metadata relating to verified CSEM reports processed by INHOPE are shared with INTERPOL for inclusion in its victim identification database.

Image-based Abuse Scheme

The OSA sets out a regulatory scheme for investigating and acting against complaints about the non-consensual sharing of intimate images, which the eSafety Commissioner refers to as the image-based abuse scheme.

Section 15 of the OSA defines an intimate image as an image (including moving visual images such as videos) that depicts or appears to depict a person's genital or anal area (including when covered by underwear), or a person's breast(s) if the person identifies as female, transgender or intersex, in circumstances in which an ordinary reasonable person would reasonably expect to be afforded privacy. Material is also an intimate image if it depicts a person in certain forms of private activity (for example, in a state of undress, using the toilet or showering) in private circumstances. In cases where a person's cultural or religious background involves the wearing of certain religious attire, an image will be an intimate image if it shows that person without the attire in a private setting.

There will be a contravention of the OSA when a person posts or threatens to post intimate material without consent. Under the OSA, consent cannot be given by a child under the age of 18. To be captured within the image-based abuse scheme, material must be posted on (or the threat must relate to) a social media service (such as Facebook), a relevant electronic service (including messaging services such as WhatsApp), or a designated Internet service (which includes websites) and either the perpetrator or victim (or both) must ordinarily reside in Australia.

eSafety has a number of regulatory options in relation to image-based abuse which can be directed at either the service providing access to the material or the person responsible for posting (or threatening to post) it.

We have established a close working relationship and agreed processes with our partners at the ACCCE to respond to reports to eSafety from Australian children and young people under 18 years. For example, if a person under the age of 18 reports to eSafety that they are the victim of sexual extortion or attempted sexual extortion, we typically:

- refer to the ACCCE for assessment and appropriate action
- provide the child or young person with advice about available supports, prevention, and online safety
- assist with removal action and/or report social media accounts pending ACCCE clearance.

Regulation of systems and processes

Basic Online Safety Expectations

The OSA provides eSafety with powers to require online services providers to report on the reasonable steps they are taking to comply with the Basic Online Safety Expectations (BOSE), which were determined by the then Minister for Communications, setting out the Australian Government's expectations of certain kinds of online services. No other regulator has equivalent powers.

In August 2022, eSafety issued its first notices to Apple, Meta (and WhatsApp), Microsoft (and Skype), Omegle, and Snap, requiring them to outline the steps they are taking to address child sexual exploitation and abuse on their platforms. Given the objectives of the Act are to improve industry transparency and accountability, eSafety will consider what information is appropriate to make public from these notices.

eSafety's regulatory guidance confirmed that further notices will be issued, including by using periodic reporting powers to track key safety metrics over time.

eSafety is working closely with law enforcement and the ACCCE to inform work on the BOSE.

Industry codes

The online industry is also progressing the development of new codes to co-regulate illegal and restricted online material, including CSEM.

In September 2021, eSafety published a position paper to help industry in the code development process. The paper sets out 11 policy positions regarding the design, development, and administration of industry codes, as well as eSafety's preferred outcomes-based model for the codes. The paper proposed that industry develop codes in two phases, with the first phase of codes covering measures to address most types of class 1 material and the second to cover certain types of online pornography that would be class 1 and all class 2 material.

Industry has consulted publicly on the first phase of draft codes and is due to provide their codes to the eSafety Commissioner in November 2022. The eSafety Commissioner will decide whether the codes provides appropriate community safeguards. If an industry code does not provide appropriate community safeguards, the eSafety Commissioner is able to determine industry standards.

eSafety can provide further information to the Committee as the code development process continues.

The global problem of child sexual exploitation

As noted in our previous submission, the scale and scope of child sexual exploitation in the current online environment is staggering, and is not limited to the 'dark web'.

eSafety has handled more than 90,000 complaints about illegal and restricted online material since 2015, the majority involving CSEM, with numbers surging since the start of the COVID-19 pandemic. This sustained, global growth is often outstripping capacity to respond, and is an issue of worldwide concern.

UK’s Internet Watch Foundation

In 2021, the UK Internet Watch Foundation (IWF) assessed 361,062 reports and 7 in 10 (252,194 reports) of those led to online material depicting children being sexually abused. Of these, 182,281 URLs contained images or videos of ‘self-generated’ material.

‘Self-generated’ child sexual abuse material is created by the child depicted in the material using webcams or smartphones and then shared online via a growing number of platforms. In some cases, children are groomed, deceived, or extorted into producing and sharing a sexual image or video of themselves. The images are created of children often in their bedrooms or another room in a home setting. With much of the world subject to periods of lockdown at home due to COVID-19, the volume of this kind of online material has only grown.

Canadian Centre for Child Protection

eSafety also works with The Canadian Centre for Child Protection (C3P), whose Project Arachnid activities led to 6 million images and videos of child sexual exploitation being removed from more than 1,000 electronic service providers across more than 100 countries worldwide.

Almost 85% of the images identified through the program relate to victims that are not known to have been identified by law enforcement agencies. We have contributed to the Arachnid program through classification and verification of detected CSEM images, helping accelerate Arachnid’s automated removal of CSEM at-scale.

INHOPE

During 2021, the INHOPE network exchanged reports about nearly one million URLs depicting suspected CSEM. 82% of content URLs were unknown in 2021. This figure was 39% in 2020. 96% of the content showed the abuse and exploitation of girls, and 82% of all reported CSEM involved the abuse or exploitation of pre-pubescent children. More than 75% of content reported as being provided from Europe was hosted in the Netherlands.

The data shows that child sexual exploitation is a global challenge that requires concerted and collaborative responses. Equally, the actions of other governments and regulators can improve online safety for Australians. In addition to engaging with hotlines, eSafety actively participates in global alliances and initiatives to mobilise and coordinate governments, regulators and international stakeholders to eradicate CSEM.

WeProtect Global Alliance

The eSafety Commissioner has served on the WeProtect Global Alliance Board since 2019. In 2022, we joined the newly established WeProtect Global Taskforce on Child Sexual Abuse Online. The Taskforce promotes improved cooperation and collaboration among governments and will:

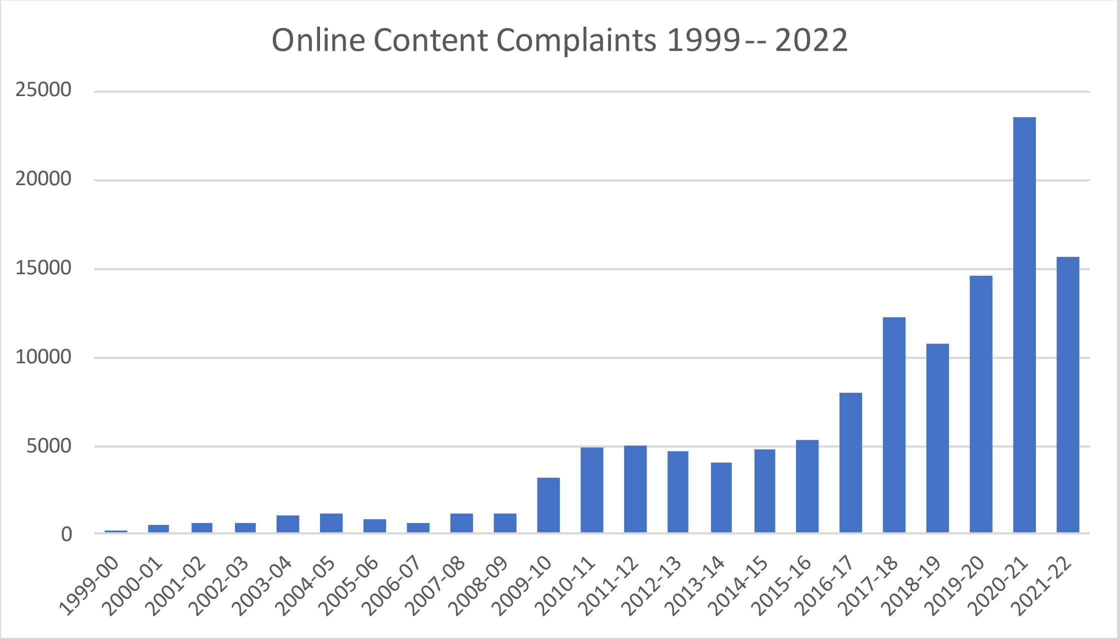
- develop and drive a global coordinated response to child sexual abuse online
- secure engagement at national, regional, and global levels
- showcase progress and champion best / emerging practice
- influence and contribute to key WeProtect Global Alliance products and membership commitments.

Global Online Safety Regulators Network

In addition, in late 2022, eSafety commenced leading work to create a Global Online Safety Regulators Network to promote cooperation and collaboration among online safety regulators. Other founding members include the Broadcasting Authority of Ireland, Fiji’s Online Safety Commission and the UK regulator, Ofcom. The Network will be officially launched in November 2022.

Complaints about CSEM made to the eSafety Commissioner

Over more than 20 years of the Online Content Scheme's operation, complaints about illegal and restricted online material by the public have seen a steady increase. During the first full year of the Scheme's operation, 201 public reports were received. In financial year 2021/22, eSafety received more than 15,600 public reports. The 2020/21 financial year saw a sharp increase in reports believed to be the result of increased internet usage during the Covid-19 pandemic. The 2021/22 figures indicate a growth in report numbers more in line with pre-pandemic increases, explaining the decrease of approximately 34% on the previous financial year. Overwhelmingly, public reports concern CSEM.



Over time, eSafety has observed a distinct shift in the nature of CSEM identified through regulatory investigations, and the nature of hosting by industry. Images and videos are far more likely to have been produced by children and young people themselves, often involving explicit sexual posing and sexual touching. This type of content appears in substantial volumes on websites and forums catering to those with a sexual interest in children, and appears to often have been produced as a result of the child being threatened or manipulated by an adult.

Increasingly, websites that contain CSEM are hosted by network providers that deliberately obscure their corporate footprint. This obfuscation can be achieved by providers registering company details in foreign jurisdictions, distributing registration across jurisdictions, and deliberately undermining the integrity of the global WHOIS database. Some providers openly market themselves as being 'bulletproof' implying that they are resistant to takedown and disruption and with a high tolerance to hosting illegal content. Removal of CSEM by INHOPE members, industry and law enforcement can be complicated by these tactics.

Image-based abuse complaints

Young reporters

About 25-30% of reports about image-based abuse are made by those aged under 18 years. Most under-18 reporters are aged between 13 and 17 years, with only a small percentage of reports from children (7%) under 13 years.

Of the reports received from under 18s, most concern sexual extortion and only 12% concern peer-group sharing. Young reporters are typically coerced into sharing images of themselves by adult offenders, who are often pretending to be young people. Once a young person has sent an image to this type of offender, threats to share their images are received and demands are made, usually for payment, but also for further images.

Our response

We encourage Australians under the age of 18 years experiencing this form of harm to report directly to the ACCCE. We have also developed internal procedures which ensure eSafety is a safe place for children and young people to come for help with these matters. These procedures align with our obligations to provide relevant information to police, including to the ACCCE.

Once a complaint about image-based abuse has been made, we manage risks to the relevant child or young person by ensuring that they cease all contact with the offender and are supported. We work with the relevant online platform to have the child's image and/or the offender's account removed (in consultation with the ACCCE).

Since the image-based abuse scheme commenced under the now repealed *Enhancing Online Safety Act 2015*, eSafety has alerted social media services to the misuse of over 1,800 accounts involved in the sexual exploitation of a child or young person, with services disabling over 80% of the accounts reported. We also refer children and young people to Kids Helpline for counselling and support.

We alert social media providers to key indicators (including the ease with which offender accounts proliferate) and are focused on the potential strength and impact of our systemic regulatory tools, including the BOSE and the draft industry codes.

Where peer-group sharing is relevant to a report, we have found that a law enforcement approach is not always a preferable option for resolution. While these matters are typically reported to police by either school staff or parents, police for a number of reasons do not always elect to prefer charges. We typically address these type of matter by:

- reporting accounts that have shared, or threatened to share, intimate images to the social media service
- giving advice on how the victim can screenshot evidence and block accounts
- providing safety advice regarding privacy settings and deleting all friends/followers who are not known and trusted offline.

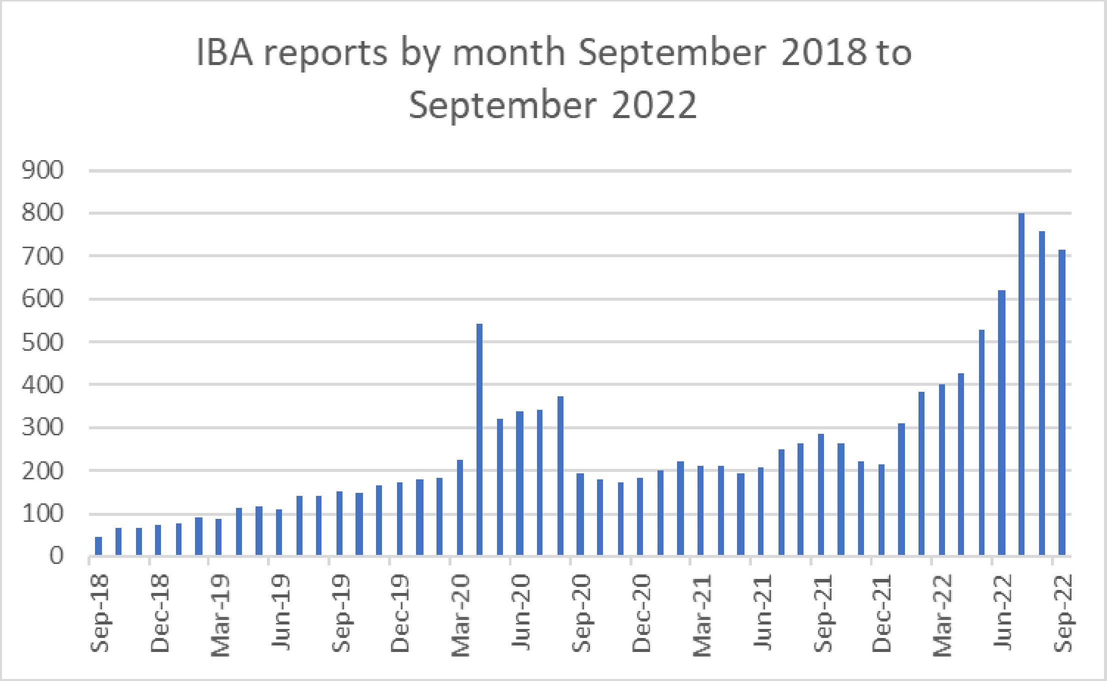
We may also:

- liaise with schools if they are in a position to help resolve the incident relating to cyberbullying
- speak with police if they are already involved or ought to be involved
- take remedial action.

IBA reports

eSafety has received more than 12,600 reports about image-based abuse over the life of the civil penalties scheme.

Almost 50% of all reports have been received in the last 12 months alone. In 2022, there has been a sharp rise in the number of sexual extortion reports to eSafety. Authorities globally are seeing a significant increase in offshore criminal syndicates targeting children and young people (mostly male) with threats to share their images in exchange for payment.



Our research

eSafety's research shows that Australian teens are exposed to a range of risks and threats online. Our February 2022 research found that many children aged 8-17 years have had contact with a stranger online or have been treated in a hurtful way online. The majority of young people aged 14–17 years have had exposure online to some form of potentially negative content, as well as to sexual material.

Research published by eSafety in 2021 has also found that while many teens take some form of action against the unwelcome contact, less than half mention it to family or friends (43%) or report it (40%). Online safety information is valued by teens, with three-quarters wanting information about issues such as how to block bad actors, how to support friends in trouble, and how to report negative online experiences.

All of this makes clear that the prevalence and accessibility of CSEM online is a challenge that goes well beyond law enforcement. Instead, addressing the many elements that enable the online sexual exploitation of children demands a whole-of-government, whole-of-community approach that reaches across borders and jurisdictional limits.

The role of technology providers in assisting law enforcement and governments

Industry policies

Most mainstream online services have policies, terms of use or community standards prohibiting child sexual exploitation and abuse on their platforms. When they become aware of such content, mainstream services which are subject to US federal law typically remove it, disable the relevant account, and report it to the US National Centre for Missing and Exploited Children (NCMEC). The NCMEC forwards the reports to law enforcement agencies around the world, including the AFP.

According to the NCMEC, 29.1 million CSEM reports regarding social media were made in 2021. Only 0.8% of these reports came from members of the public. The vast majority came from online services, most of which check for this content using well-established photo matching technologies. These technologies involve checking if content on a service matches the unique 'digital fingerprint' of previously confirmed CSEM. The error rate of these technologies is designed to be between one in 50 to 100 billion. Services then report this content to designated organisations such as NCMEC, enabling material to be tagged, traced, and removed.

Services can also detect and action CSEM through Trust and Safety teams and automated tools. Some of this work is proactive, such as scanning content for potential CSEM at upload, and some is reactive, such as providing reporting mechanisms for users to notify potential CSEM to the service.

As eSafety's previous evidence highlights, the effectiveness of these measures varies across services, as does the level of investment, innovation and collaboration undertaken to combat CSEM. Another variable element is the level of transparency that services provide in relation to these efforts. There are several groups currently working to drive up industry practices and standards through collective action. These include the industry-led Technology Coalition, which recently released its Voluntary Framework for Industry Transparency, and the cross-sector, multi-stakeholder WPGA, mentioned above. However, in eSafety's experience to date, voluntary transparency initiatives have had limited uptake, or are anonymous and aggregated such as the Technology Coalition's current reports.

As noted above, eSafety recently issued notices to seven online providers to improve transparency and accountability and lift the hood on what services are, or aren't, doing to prevent child sexual exploitation and abuse.

In our prior submission, we outlined some of the industry-led initiatives which have had a tangible impact on the ability of offenders to find, share and store CSEM online.

Key Challenges

Encryption

Photo-matching technologies that detect illegal material by proactively scanning, monitoring and filtering user content currently are not applied to systems that use end-to-end encryption (E2EE). Because of this, E2EE can facilitate the production and exchange of CSEM.

If major social media platforms increasingly employ E2EE on their services, for example Meta's rollout for default E2EE for all personal messages and calls in 2023, it will make investigations into serious online child sexual abuse and exploitation significantly more difficult. It will create digital hiding places, and platforms may claim they are absolved of responsibility for safety because they cannot act on what they cannot see. NCMEC estimates that more than half of its 2021 reports would cease to be possible if platforms transitioned to E2EE.

There are a number of developing solutions that would ensure illegal activity online can be addressed that do not compromise encryption and allow lawful access to information needed in serious criminal investigations. Emerging solutions include using implementing proactive detection tools at transmission, at the device level (as Apple is exercising with its safety prompts for children sending/receiving nudity in iMessage, launched in April 2022 in Australia).

Immersive technologies

eSafety has significant concerns about the use of immersive technologies as a tool for online child sexual abuse, including through the use of augmented reality (AR), virtual reality (VR) such as the metaverse, mixed reality (MR) and haptics.

These environments can provide hyperrealistic experiences that can be exploited by predators as a way to meet and groom children and young people for sexual abuse. For example, sexual assaults might be experienced virtually through a haptic suit, augmented realities could be used to fake a sexually explicit three-dimensional image or video of a real person and interact with it, without their consent, and a virtual experience may feel private because you are physically isolated, but if you use it to create an intimate image or video the file could be livestreamed, stored, stolen, or shared without consent.

eSafety has not yet received any complaints or reports of harms inflicted via augmented, virtual, or mixed reality or haptics that are addressable through our complaints-based schemes. However, we expect we may soon receive reports of immersive technologies being involved in image-based abuse and the production and spread of CSEM.

Addressing challenges through international engagement

The key challenges outlined here are not unique to Australia. It is increasingly understood that voluntary actions alone against CSEM have proven insufficient and we are seeing new legislation progress in Europe, Canada, Singapore, and the UK.

For example, in May 2022, the European Commission published its proposed Regulation to prevent and combat child sexual abuse. The proposed legislation will require providers to detect known CSEM, and to work towards the creation of a European Centre to prevent and counter child sexual abuse, similar to the role of the ACCCE. This initiative followed a visit from Members of the European Parliament to Australia in February 2022, where eSafety shared detail on our operating model, enabling legislation and a visit to the ACCCE.

Protection of children online is now a main feature in many UN and multilateral forums. eSafety has worked with the Department of Foreign Affairs & Trade to advance Australia's core priorities through the Commission on Crime Prevention and Criminal Justice (CCPCJ) to countering cyber-crime, including the online abuse and exploitation of minors in illegal activities.

Recognising the scale and volume of the issue of CSEM, eSafety is part of a cross-agency, cross-sector, and multi-jurisdictional effort – one which has grown increasingly effective over recent years.

AFP
AUSTRALIAN FEDERAL POLICE

6 October 2022

Senator Helen Polley
Committee Chair
Parliamentary Joint Committee on Law Enforcement
PO Box 6100
Parliament House
Canberra ACT 2600

Via email: le.committee@aph.gov.au

Dear Ms Polley,

Re: Continuation of inquiry into law enforcement capabilities in relation to child exploitation

1. The Australian Federal Police (AFP) welcomes the opportunity to provide the Parliamentary Joint Committee on Law Enforcement (PJCLE) additional information to inform its inquiry into law enforcement capabilities in relation to child exploitation.

2. For reference, attached is AFP's submission from August 2021 outlining the AFP's role in addressing child exploitation and providing operational insights on the threat environment, emerging trends, and legislative gaps. This letter is designed to be read alongside the previous submission and includes updated operational trends, statistics and advice.

Operational updates

3. In the 2021/22 financial year, the AFP charged **221** offenders with **1,746** charges for child abuse related offences. In this time period, the Australian Centre to Counter Child Exploitation (ACCCE) Child Protection Triage Unit received more than **36,000** reports of child sexual exploitation, an increase of 62% from the previous financial year.

ACCCE/AFP Statistics	2018/19 FY	2019/20 FY	2020/21 FY	2021/22 FY
Incoming reports of child exploitation received	14,285	21,668	22,600	36,660
Arrests (including summons, court attendance notices, etc.)	74	161	235	221
Charges laid	372	1,214	2,772	1,746
Victims identified	38	37	184	170
Children removed from harm	72	134	232	79

Note: as in the August 2021 submission, these statistics include online and contact offending.

4. These statistics reflect major AFP operations from the 2021/22 financial year including Operation Tatsuta, an operation coordinated by the South Australian Joint Anti-Child Exploitation Team (JACET) in collaboration with AFP International Command, Philippine

Internet Crimes Against Children Centre, the Philippine National Police and the AFP Criminal Assets Confiscation Taskforce (CACT).

Case study – Operation TATSUTA

Operation Tatsuta resulted in the successful prosecution of an Adelaide man who was actively participating and directing the live online child sexual abuse of 13 child victims by five adult facilitators located in the Philippines. Through information provided by the AFP, the PNP arrested five facilitators of live online child sexual abuse (LOCSA) and rescued 15 victims of sexual exploitation.

The AFP CACT commenced civil proceedings against the offender, resulting in a restraining order being issued against his residence in South Australia, the first time this has occurred against a child sex offender. This action resolved with the offender paying $165,000 to the Commonwealth. In August 2022, the offender was sentenced to a total of 16 years' imprisonment, with a fixed non-parole period of 10 years.

5. The joint AFP Operation Tamworth/Western Australia (WA) Police Operation Palomar, went to resolution in September 2022 (outside of the 2021/22 financial year – and is therefore not included in the above statistics). The WA Police led operation involved AFP and Australian Border Force, and sought to target the manufacture, distribution and possession of child exploitation material in the state of WA.

6. As at 15 September 2022, the joint operation has resulted in 45 people being charged in WA with 149 offences, 35,222 images and videos of child exploitation material being seized, and three victims being identified and rescued from ongoing harm.

Newly emerging trends and changes

Increase in extortion-based behaviours

7. As identified in the AFP's previous submission, our operational teams continue to encounter an increase in the application of technological advancements to offending, self-generated sexual content, and the proliferation of live online child sexual abuse.

8. The AFP is also seeing an increase in online sexual extortion. Also referred to as 'sextortion', this offending refers to a serious form of blackmail where an offender coerces a victim to self-generate child abuse material and then threatens to share that material unless their demands (sometimes for money or more images) are met.

Case study – Operation HUNTSMAN

ACCCE-led Operation Huntsman is an internally generated operation in response to material identified relating to the international sextortion of Australian children. It was initiated due to a significant and sustained rise in numbers of sextortion referrals received by the ACCCE. Between April and August, the number of victim reports received by ACCCE was 396. Extrapolate from that number, with our understanding that sextortion is substantially underreported, the number of victims could be much greater and exceed well over a thousand.

Operation Huntsman has identified that offshore persons are blackmailing adolescents via social media platforms using real or doctored images of them in compromising positions. This material is then used to coerce the children into providing payment or, in some circumstances, new material.

9. Where offenders threaten children for the purposes of obtaining new child exploitation material, the AFP would seek to pursue charges under *Criminal Code Act 1995* (Criminal Code) sections 474.17 and 474.17A in the first instance. These offences carry a maximum penalty of imprisonment for five and six years respectively, which is not always reflective of the seriousness of the offending and the fear invoked in victims.

10. Law enforcement is working domestically and internationally to address this trend. The AFP and ACCCE developed an awareness and education package, including a new *ThinkUKnow* education resource aimed at teenagers from 13-17 years old on how to recognise sexual extortion and how to get help; a media and social media campaign; and video message to encourage young people to report to police. In a four-day period, it is estimated that the campaign reached 7.5 million people.

New and ongoing initiatives

ACCCE Animations

11. The ACCCE has launched a series of new online animations to raise awareness and prevent online child sexual exploitation.

12. Through market research and consultation with stakeholders, the ACCCE identified that confusion still exists in the community around what constitutes online child sexual exploitation, where to report matters, and the work of the ACCCE. The animations '*What is the ACCCE, What is Online Child Sexual Exploitation* and *How to Report Online Child Sexual Exploitation'*. These animations seek to support families to actively engage in conversations with their children, following ACCCE research illustrating that only 52% of parents talk to their children about online safety.

Child Protection Children's Book

13. The ACCCE undertook market research in 2019 into the current awareness, perceptions and attitudes of online child sexual exploitation, which recommended a requirement for resources and tools for information and support to complement education activities.

14. Together, the AFP and ACCCE have developed a children's picture book titled "*Jack Changes the Game*", designed for parents, carers and teachers to start conversations with primary school children in Year 1-3 (5–8 years old) about being safer online. The picture book aims to help children recognise the signs of online grooming, how to get help and the importance of reporting.

15. The book is supported by a *ThinkUKnow* learning package, including lesson plans and home activities to assist in reinforcing key concepts at home and in the classroom. To develop the book, the AFP and ACCCE established a highly credible academic advisory reference group with leading experts in education and child protection. The reference group has been engaged throughout the project from conception, storyline and illustrations.

16. The book was launched at the ACCCE on 4 October 2022. The AFP and ACCCE will work with partners to distribute the book. For example, Australia Post will deliver copies to every primary school in Australia.

Travelling Child Sex Offender Campaign

17. In November 2022, the ACCCE will be launching a pilot awareness and deterrence campaign at Brisbane International Airport, targeting travelling child sex offenders. This ACCCE priority program has been designed to address the increasing prevalence of sexual exploitation of children in the context of travel and tourism, which is strongly linked to online child exploitation. Following the pilot in Brisbane, the ACCCE will look to roll out the campaign nationally in early 2023.

ThinkUKnow program – updates and national training rollout

18. The AFP leads *ThinkUKnow*, an evidence-based education program to prevent online child sexual exploitation.

19. The AFP undertook updates to the *ThinkUKnow* presentation suite for 2022, to reflect trends and issues based on real reports and investigations. This package was released in April 2022 to coincide with the beginning of Term 2.

20. Between April – July 2022, the AFP delivered the updated *ThinkUKnow* presentation training to AFP, State and Territory police and industry presenters across Tasmania, ACT, South Australia, Northern Territory, Western Australia, Queensland and New South Wales, including metropolitan and regional areas, as well as hosting virtual training sessions in Victoria.

21. Since the commencement of the updated *ThinkUKnow* program, 350 members have attended face-to-face training and 106 members participated through virtual sessions.

Victim Identification Taskforces and Training

22. Between May 2021 and May 2022, the ACCCE Victim Identification Unit facilitated three victim identification taskforces (VIDTF). The VIDTF's bring together state and territory law enforcement partners to review material and work collaboratively towards identifying victims. Across the three VIDTFs, more than 10,500 media files were contributed to the INTERPOL International Child Sexual Exploitation (ICSE) database, 100 new series were created on ICSE, and additional material was contributed to 46 existing victim series on ICSE. Over the course of the VIDTFs, 30 victims have been identified and more than 60 victims and/or offenders referred for investigation.

23. In November 2021, the ACCCE launched an online Victim Identification Awareness training package, which has now been accessed by more than 200 members from all policing agencies in Australia. Law enforcement representatives from Europol, INTERPOL, Denmark, Norway, New Zealand, United Kingdom and the United States have also completed the training course.

24. In May 2022, the ACCCE facilitated the first national specialist victim identification training, during which 11 victim identification members from across Australia and New Zealand developed their skills in analysing media to identify child victims.

Child Sexual Exploitation Regional Dialogue

25. In May 2022, the AFP led the Child Sexual Exploitation Regional Dialogue in Siem Reap, Cambodia. This dialogue saw law enforcement representation from 14 countries alongside non-government organisations and locally based foreign agencies. The dialogue has highlighted the importance of collaboration between foreign law enforcement to improve investigation techniques and information sharing between partner agencies.

Wellbeing of Child Protection Operation and ACCCE members

26. The AFP and ACCCE consistently seek to employ best practice when providing psychological care and supporting the wellbeing of our people. The ACCCE building was designed as an integral part of the wellbeing plan, encouraging members to utilise the collaboration and breakout areas to interact and step away from high risk explicit material exposure areas. The building has two floors which have strict access control measures in place to minimise potential exposure to explicit material. The operational floor has physical protective measures including viewing controls, tint and strategic placement of monitors to avoid accidental exposure. Other measures include the introduction of wellbeing dogs, where members' dogs visit the ACCCE building on Fridays, and other recognised support practices.

The National Strategy to Prevent and Respond to Child Sexual Abuse

27. The First Commonwealth Action Plan delivers $35.4 million over 4 years to the AFP and the National Action Plan delivers $22.5 million over 4 years to the AFP. AFP-led measures include a national enhancement of victim identification, forensic triaging capability, expanding AFP international operations and enhancing child protection investigations in the Northern Territory. The Child Protection National Strategy Implementation and Performance Review Board (IPRB) [SES1] has met bi-monthly since November 2021. The IPRB determines how AFP can implement initiatives to ensure we meet the National Strategy requirements and to enhance the AFP's collective efforts. The Child Protection National Strategy Executive Review Board (ERB) [SES2] met in May 2022. This Board ensures AFP delivers on the intent of the National Strategy and aligns with the strategic direction of the AFP. AFP participates in the National Strategy Policy Working Group, which is responsible for implementing the National Strategy.

Law Enforcement partnerships

28. The Virtual Global Taskforce (VGT) is an international alliance of dedicated law enforcement agencies and partners, working together to reduce the global threat from, and vulnerability of children to, online sexual abuse and other forms of transnational child sexual offending. The AFP are key members of the VGT Board of Management (BOM), which comprises of a coalition of international law enforcement agencies. The VGT was established in 2003 as a direct response to lessons learned from investigations into online child sexual abuse around the world. The child sexual abuse threat is a global one and the VGT seeks to deliver innovative, global strategies in order to safeguard children online. The AFP are expected to outline initiatives to investigate, deter and prevent child sexual exploitation and highlight our contribution to international collaborative efforts. Key topics in the VGT BOM will include operational techniques and tools as well as ongoing international operations. There will be an opportunity to discuss operational architecture, capacity building and how partnerships can be strengthened and enhanced between agencies.

29. The Five Eyes Law Enforcement Group (FELEG) Vulnerable Persons Working Group (VPWG) started as a 12-month pilot, but owing to changes within the FELEG it is now a "Community of Practice" rather than a working group. The VPWG has been developed to tackle the issue of live streaming of child abuse material within vulnerable populations, including current and emerging markets. The end goal is to leverage shared knowledge and capabilities of individual FELEG agencies to develop best practice and a collaborative approach to transnational investigations. The group is still in the start-up phase, with a live streaming assessment ("deep dive") in the final stages. The assessment is being put together by National Assessment Centre (NAC) of the NCA with support from the international community for the Criminal Intelligence Advisory Group (CIAG) and will inform the direction of the group once finalised.

Gaps in the existing framework

Improving use of community and victim impact statements

30. In addition to the issues flagged in the AFP's 2021 submission, the AFP and ACCCE see benefit in clarifying the existing *Crimes Act 1914* (Cth) Part IB application to victim impact statements to consider the significant amount of harm and re-victimisation that the victims of child exploitation face and permitting the submission of community impact statements.

31. For example, we see benefit in permitting the submission of statements from victim-survivors depicted in material found in the offender's possession, including where the offender is not responsible for producing, procuring or soliciting that material directly from the victim (i.e. the material was already in circulation and the offender obtained it without contact with the victim). Enabling the submission of statements in this instance recognises that the ongoing existence and sharing of the child abuse material contributes to harm and that individuals are often re-victimised when their material is shared online.

32. The AFP also supports permitting community impact statements (also known as group impact statements) on behalf of victim-survivors depicted in child abuse material available online, none of whom are necessarily depicted in the material in the offender's possession. For example, convictions for possessing child abuse material obtained using a carriage service do not require a complainant and a community impact statement could detail the impact that online child sexual abuse has on victims.

33. In 2010, South Australia (SA) became the first State to permit a community impact statement being provided to the court. This legislation provides for two types of statements to be utilised during sentencing proceedings; the first being a 'Neighbourhood Impact Statement' and the second being a 'Social Impact Statement'.

34. Since 2021, AFP as part of the SA JACET has partnered with the South Australian Commissioner for Victims' Rights to develop and utilise Social Impact Statements for investigations undertaken by the SA JACET.

35. These statements are designed to give victims and the community a voice within the judicial process and to inform the court of the impacts of offending on the individual and the wider community.

36. SA is currently the only jurisdiction in Australia permitting the use of these statements. AFP's experience with the SA JACET highlights the benefits of these types of statements being used to represent the victim and the community interests.

Conclusion

37. We hope this additional information assists the Committee in understanding the continually evolving threat environment and updates on measures and initiatives since the AFP's last submission. The AFP welcomes an opportunity to appear before the Committee to expand on this submission (as well as the information provided in the AFP's 2021 submission) if needed.

Yours sincerely,

Lesa Gale
Performing the duties of Deputy Commissioner Operations

AUSTRALIAN FEDERAL POLICE

Parliamentary Joint Committee on Law Enforcement

Inquiry into Law Enforcement Capabilities in Relation to Child Exploitation

25 August 2021

Submission by the Australian Federal Police

Introduction

1. The Australian Federal Police (AFP) welcomes the opportunity to make a submission to the Parliamentary Joint Committee on Law Enforcement (the Committee) Inquiry into law enforcement capabilities in relation to child exploitation.

2. The threat to children, those most vulnerable in our community, is evolving. Operational experience has shown that the borderless crime of online child sexual exploitation is progressively difficult to tackle, especially as the use of anonymising technology and encrypted platforms become increasingly prevalent.

3. The AFP is at the forefront of combatting child exploitation in Australia, and leads the coordination of national efforts to uncover and locate child sex offenders who engage in all forms of exploitation and abuse.

4. The AFP is not only responsible for the operational response and investigation of offenders coordinated by AFP Child Protection Operations (CPO) through the Joint Anti-Child Exploitation Teams (JACETs) and the Northern Territory Child Abuse Taskforce (NT CAT), but is also a leader in prevention and education initiatives such as the AFP *ThinkUKnow* program, and strategic leadership, research and collaboration through the AFP-led Australian Centre to Counter Child Exploitation (ACCCE). A detailed overview of the ACCCE is below at paragraphs 40-50.

5. Child exploitation is a high volume crime, requiring substantial resourcing and the use of all available legislative and technological capabilities to combat. Through AFP's extensive operational experience, a number of gaps have been identified in the existing frameworks, which are detailed further in this submission. Addressing these gaps will further assist the AFP and our partners to tackle child exploitation. This submission was prepared in consultation with the AFP's close partner, the Australian Criminal Intelligence Commission (ACIC) to focus on operational experiences in combatting child exploitation. The Department of Home Affairs has also prepared a submission, which provides policy context. The AFP recommends the submissions be read alongside one another to provide a full picture of the Commonwealth response to the criminal environment.

Nature and Extent of the Threat: Child Exploitation

Online child exploitation and the impact of COVID-19

6. Child exploitation has unfortunately been a considerable problem for law enforcement authorities for an extensive period of time. Since the onset of the COVID-19 pandemic, and as a result of the growing number of households spending considerably increased time online (with sometimes limited security measures) the availability and access to children online has increased.

7. In 2020/21, the AFP arrested 235 offenders, laid 2,772 charges, identified 184 victims and removed 232 victims from harm. This is a significant increase from previous years as per below.

ACCCE/AFP statistics	**2018/19 FY**	**2019/20 FY**	**2020/2021**
Incoming reports child exploitation received	14,285	21,668	22,600
Arrests	74	161	235
Charges laid	372	1,214	2,772
Victims identified	38	37	184
Children removed from harm	72	134	232

Note: Stats include online and contact offending.

8. A number of means can be attributed to the significant increase of reports, arrests, charges laid, victims identified and children removed from harm in comparison to previous years. An increase in victim identification capability and the ACCCE's Victim Identification Units review of the International Child Sexual Exploitation (ICSE) database material has attributed to some of these increases, in conjunction with national collaboration and coordination efforts that have seen an increase in victims being uploaded to the ICSE.

9. The AFP and ACCCE have observed the emergence of a number of child abuse forums established as a result of COVID-19 stay at home measures. These forums now include more than 1,000 members combined and specifically provide advice on how to establish online relationships with children in the COVID-19 environment.

10. The use of carriage services contributes heavily to the proliferation of child exploitation. Between 01 July 2020 and 31 June 2021, the most commonly used Commonwealth offences have been:

Offence	Counts
Criminal Code section 474.22 – using a carriage service for Child Abuse Material	494
Criminal Code section 474.22A – Possessing or controlling child abuse material obtained or accessed using a carriage service	264

11. Some material uncovered by police can be extreme – depicting children, including very young children, being subjected to physical and sexual abuse, torture and cruelty.

Application of technological advancements to offending

12. Online child exploitation continues to be difficult to track and investigate. This complexity is compounded by wide-scale adoption of encryption, anonymising technologies, streaming services and 'pay-per-view' models, and use of virtual

currencies to obfuscate law enforcement detection. However, online child abuse offenders do also operate on the 'clear-net', and law enforcement continues to observe offenders using non-encrypted communication channels. It is important to note that the vast majority of reports received by NCMEC are from clear net electronic service providers, which continues to demonstrate the prevalence of online child exploitation on clear net platforms.

13. Law enforcement continues to observe offenders using non-encrypted communications channels, such as web forums and social media chat functions. Offenders share insights, tips and protocols with each other, with the aim of preventing or defeating law enforcement detection. It is the case that this communication is, at times, not in the encrypted communications space.

14. The hosting, sharing and distribution of child abuse material is increasingly occurring on dark web hidden services, which require specialised browsers and other anonymising software to access. These technologies are free or low cost for perpetrators to use, yet make a significant impact on the ability for law enforcement to detect and access.

15. The scale of offending on such platforms is significant and many services have tens of thousands of users across the world. Offenders using such platforms are cautious of law enforcement, and often produce and share 'how to' guides to assist perpetrators on avoiding law enforcement detection alongside instructional guides for producing child abuse material. Traditional law enforcement techniques struggle to address the scale of this problem.

16. Maliciously designed remote administration tools (RATs) are a common form of malware intended to provide an offender with control over a victim's computer. Though RATs have legitimate uses, they can be used to facilitate the commission of child exploitation offences. For example, through unauthorised access to a child's account to assume their identity and obtain exploitation material from others, or the activation of a victim's web camera to create child exploitation material.

17. Overall, the volume of child abuse material facilitated by and shared on the dark web is difficult to quantify. However, since the beginning of the COVID-19 pandemic, the ACCCE has identified over **800,000** registered accounts utilising anonymised platforms such as the dark web and encrypted apps, solely for the purposes facilitating child abuse material.

18. To ensure the protection of children during the COVID-19 pandemic, the AFP bolstered resources within the ACCCE Child Protection Triage Unit to address the increase in referrals received.

Self-generated sexual content

19. Children and young people are being targeted by online child sex offenders through social networking, image, video and instant messaging applications to self-produce online child sexual exploitation material.

20. Self-generated content can occur for a number of reasons, including but not limited to, consensual sexting, feeling pressured or coerced, sexual extortion, financial gain

and in some instances children are being groomed and blackmailed to produce more extreme material.

21. In cases of sexual extortion, offenders are manipulative and make the victim feel there is no way out of the situation. Offenders employ fear, coercion and manipulation tactics to continue to force the victim produce more material, including threatening that if the victim does not comply, previous material will be shared. Offenders exploit young victims' feelings that they have done something wrong and will be reprimanded by parents or carers and even prosecuted by the law if their actions are discovered.

22. Law enforcement face challenges in dealing with self-generated content as it is a highly stigmatised issue and in the majority of cases parents and carers are unwilling to discuss the topic with their children or with others; which can adversely affect the number of cases reported.

23. Research conducted by the ACCCE indicates that 21% of parents and carers thought the topic of self-generated material to be too sickening or disgusting to think about, 21% of parents thought that online child sexual exploitation could not happen in any form to their child and 15% of parents and carers reported that if their child was exploited online they would be too embarrassed to discuss this with others.

24. The ACCCE Prevention and Engagement team are innately aware of the challenges faced with the issue of self-generated content. The AFP, through the *ThinkUKnow* program, takes an educative approach to addressing the issue of self-produced child abuse material. The AFP believes it is important to empower young people to make informed decisions to promote their safety, and the safety of those they interact with, as well as encouraging help seeking behaviours. With a crime prevention focus, *ThinkUKnow* engages with educators, parents, carers and children, supporting the community to work together with police in reducing the incidences of online child sexual exploitation.

25. Further to the above the ACCCE is working on a number of projects to address these issues and fill the gaps. This includes the soon to be launched '*Stop the Stigma*' national awareness campaign, which the ACCCE has worked on in conjunction with ACCCE Prevention Working Group partners.

Live Online Child Sexual Abuse (LOCSA)

26. The AFP is aware that in the current online-heavy operating environment there has been demand for consumption of Live Online Child Sexual Abuse (LOCSA), also known as 'Live Distance Child Abuse'. This can be largely attributed to the limitations of international travel and the consumption of online child abuse material being seen as a 'safer' way to offend.

27. This phenomenon is distinct from other forms of child abuse material, as LOCSA is primarily executed through livestreaming. No electronic trace is left on the device or remote servers except for session logs or data usage statistics, and law enforcement are often only alerted to the crime where the offender captures and uploads screenshots or video to other platforms. Although LOCSA can occur in various countries, facilitators often come from Southeast Asia. Countries in this region with

high levels of poverty, high-speed internet connections, English language proficiency, and advanced remittance services leave facilitators well positioned to profit from this abhorrent offending.

28. Such criminal activity is captured under section 474.24A of the *Criminal Code 1995* (Criminal Code) which captures conduct where children are coerced into participating in sexual activities (performed alone or with others) which are broadcast live over the internet for criminals to watch remotely (using a carriage service). Consumers paying for the abuse to be broadcast often direct the facilitator to perform requested acts on a victim.

29. Due to the methodology associated with this offending, law enforcement and partners only have visibility of a fraction of the offending in this space and are required to estimate the proliferation of LOCSA. As a result of the relationships formed between the offenders (consumers and facilitators) and the victim, there remains a risk that the consumer may travel to offend in person against the victim or other children.

Travelling child sex offenders following re-opening of international borders

30. While the COVID-19 pandemic has affected the ability of Australians to travel freely, the threat posed by travelling child sex offenders is significant.

31. In 2017, the Australian Parliament passed world-leading reforms in the *Passports Legislation Amendment (Overseas Travel by Child Sex Offenders) Act 2017* that allow for the cancellation of passports held by registered sex offenders to prevent them from travelling overseas.

32. Due to COVID-19 international border restrictions, the AFP have not charged any registered child sex offenders for attempting to travel without permission between 01 July 2020 and 30 June 2021.

33. However, the AFP charged 4 individuals with 44 counts of engaging in sexual activity with a child outside Australia contrary to section 272.9(1) of the Criminal Code in the 2020/2021 financial year.

34. The AFP have issued **101** notifications to foreign law enforcement agencies relating to the travel of registered child sex offenders in the last financial year, down from previous years (187 in 19/20 and 347 in 18/19) due to the international border closure. The majority of alerts were for travellers being deported or who have renounced Australian citizenship.

35. The total number of notifications may not fully represent the total number of child sex offenders travelling, noting that the AFP may leverage its strong international relationship to engage with foreign law enforcement not captured by these statistics.

36. The AFP is cognisant that the re-opening of international borders in 2021-22 will likely result in a corresponding increase in travel overseas by child sex offenders to engage in, encourage, or benefit from sexual activity with children.

37. As the borders begin to open, the AFP will continue to engage with key partner agencies, such as Home Affairs and the Australian Border Force to prevent and

disrupt the sexual exploitation of children outside of Australia posed by travelling child sex offenders.

Human trafficking and forced marriage

38. Forced marriage remains the highest reported human trafficking/modern slavery offence type, making up approximately 35% of reports made to the AFP of human trafficking/modern slavery. The average age of victims is between 15 and 19 years.

39. During the 2020/21 financial year the AFP received 224 reports of Human Trafficking, with 79 of these reports relating to forced marriage. The number of reports relating to forced marriage in 2020/21 is less than in 2019/20 (92 report) with this slight decline being attributed to the environmental conditions caused by COVID-19. This includes the downturn in domestic and international travel and decreased presence of young persons in schools, limiting schools' ability to identify and report potential victims of forced marriage. However, the AFP remains concerned by these recent figures.

40. Though international travel restrictions have limited the opportunity to facilitate the movement of people into and out of Australia for exploitation purposes there are concerns that the COVID-19 pandemic has increased the risks within Australia. Individuals in vulnerable circumstances, including those under financial hardship and at risk of family violence, are at greater risk of exploitation.

41. The AFP's human trafficking operations have been maintained throughout the pandemic. Importantly, this has included the removal of **57** victims from harm domestically during the 2020/21 financial year and the repatriation of **one** victim who had been trafficked from Australia during international travel restrictions. The AFP works with its domestic and international partners to support the repatriation of victims from overseas.

42. Prevention and education is crucial to improving the identification and reporting of forced marriage, and reducing its prevalence in the community. Between 2013 and 2021, **46%** of forced marriage reports involved disruption or intervention strategies that prevented an offence from occurring. The AFP leverages its strong working relationships with government, industry, academia and non-government organisations (NGOs) through initiatives such as *Project SKYWARP*.

43. The AFP's *Look a Little Deeper* is a human trafficking and slavery information and awareness program for frontline police and other government agencies, with the program extending its remit to include NGOs and the Australian community in 2021. The extended version of the package is currently being developed with a specific focus on education relating to forced marriage. The package will be delivered to the community through our Community Liaison Teams (CLTs) and is the first of its kind in Australia.

44. Community engagement remains essential to addressing this crime type. The AFP, through the CLTs, has taken steps to actively engage with female community leaders to foster awareness and increase education on forced marriage. These community leaders have expressed an interest in working closely with the CLTs in

the future to prevent a broader range of criminal activity experienced within their communities.

45. In comparison, *Project SKYWARP* was a localised campaign first delivered in 2019 in partnership with Anti-Slavery Australia, the Sydney Airport Corporation and the Australian Border Force. The project involved the placement of forced marriage awareness materials in transit areas and washrooms across Sydney International Airport for a period of six months, to educate the public on the indicators of forced marriage and encouraged victims and witnesses to contact authorities for help. The materials directed people to the *My Blue Sky* website run by Anti-Slavery Australia, which provides extensive advice on forced marriage and anonymous support services to those affected.

46. Following *Project SKYWARP*, traffic to the *My Blue Sky* website increased from **5704** users in 2019/20 to **6842** users in 2020/21. The awareness campaign may also have contributed to a rise in reports of human trafficking to the AFP, which increased from **61** in 2018 to **91** in 2019, and to **92** in 2020.

AFP role in combatting child exploitation

Australian Centre to Counter Child Exploitation (ACCCE)

47. Operational since 2018, the AFP-led ACCCE is a world-class collaborative hub, bringing together law enforcement, public and private sectors and civil society, to drive a national response to deter, disrupt and prevent child exploitation, with a specific focus on countering online child sexual exploitation.

48. The ACCCE does not perform a traditional investigative function, in that it does not directly investigate or charge offenders or undertake briefs of evidence, but rather supports the investigative role and remit of the AFP Child Protection Operations, and state and territory police. The ACCCE endeavours to: reduce economic, social and individual rewards from child exploitation; reduce harm from organised child exploitation networks; enhance capability and interoperability between public and private sectors, and civil society; and enhance community confidence. AFP and the state and territory police, through the JACETs, retain the investigative authority in responding to child exploitation.

49. The ACCCE was developed out of Australian law enforcement experiencing an ongoing increase of reports relating to online child sexual exploitation in Australia. The ACCCE's foundational principle is partnership, with its four pillars being prevent, prepare, pursue and protect. Housed within the ACCCE are co-located resources from Queensland Police Service, Home Affairs (HA), Australian Border Force (ABF), AUSTRAC and the ACIC. The support received from these partners is significant. For example, in 2020 the ACIC established the Child Exploitation Intelligence Team (CEIT). The CEIT is dedicated to identifying new and emerging trends in online child sexual abuse, including livestreamed abuse. This team develops enhanced intelligence products by linking criminal intelligence, criminal history information, suspicious matter reports (SMRs) and international travel data.

50. Between 1 July 2020 and 30 June 2021, the ACCCE Child Protection Triage Unit received **22,600** reports of child sexual exploitation. Each report may contain hundreds of thousands of images of children being abused. This significant number of reports may be attributable to the increasing access globally, and growth in technology (such as faster and more available data exchanges).

51. Operation MOLTO is an ACCCE-coordinated operation as part of its role in enhancing interoperability with state and territory partners. The operation commenced in 2020, when the ACCCE was referred information from an international partner. The ACCCE conducted the initial review of the information, before a joint national operation was commenced involving the AFP and all Australian state and territory police. Through the collaborative efforts of key state and territory partners, the operational leads were dispersed across the country for investigation.

52. Initially, the operation targeted offenders sharing some of the most abhorrent child abuse material circulating online. Operation MOLTO has identified alleged offenders in all Australian states and territories, ranging in ages from 19 to 57 years old. As at 31 July 2021, a total of **100** persons have been charged with **888** offences and **30** children have been removed from harm.

53. Operation MOLTO represents a fraction of this extensive criminal environment. Each year, the ACCCE and the AFP's workload grows.

54. The AFP and the ACCCE's role is further reaching than just Australia. The AFP is committed to pursuing individuals engaged in child exploitation and contact offending even when the child victims are outside of Australia. The below statistics represent charges over the last financial year and demonstrate that the AFP will endeavour to apprehend and charge Australian citizens who engage in this behaviour regardless of their whereabouts.

Offence	Counts
Criminal Code section 273.5 – Possess, control, produce, distribute, obtain child porn material outside Australia [repealed offence – captures historical offending]	55
Criminal Code section 273.6 – Possess, control, produce, distribute, obtain child abuse material outside Australia	52
Criminal Code section 272.9(1) – Engaging in sexual activity with a child outside Australia	44

55. The ACCCE also engages in a significant body of work to spread awareness of online child sexual exploitation in Australia and internationally. For example, in March 2021, the ACCCE launched the *Stop Child Abuse - Trace an Object* initiative in Australia. Originally developed by Europol, the initiative engages with the community to assist with the identification of objects, clothing or surroundings taken from the background of child sexual abuse images and videos. The ACCCE website hosts these images and is currently

the most viewed page on the website. Since its launch the page has been viewed **51,882** which has resulted in **571** reports made to the ACCCE Victim Identification Unit.

56. In June 2021 the ACCCE, in partnership with the AFP, launched the *Closing the Net* podcast, a ten part series that highlights the work of law enforcement, government, academia, and non-government organisations. The series shares compelling insights of more than 55 people who dedicate their lives to combatting child exploitation through their work, as well as people who have committed to preventing child abuse through dedicating education and resources to the cause.

57. *Closing the Net* showcases that knowledge is power, and aims to encourage hard conversations between parents, carers, teachers and community members. It provides tips and advice around how to protect children online, and how to identify and report offensive online behaviour. The podcast has proven to have a significant impact with more than **45,000** downloads since its launch.

Joint Anti Child Exploitation Teams (JACETs)

58. The JACETs are teams comprised of AFP and state and territory police, located in all capital cities across Australia. The JACETs establish a collaborative framework for combatting child sexual exploitation in Australia and by Australians offshore. In 2020/21 financial year the JACETs finalised **155** cases in relation to child exploitation, with **63** cases remaining before the court and **7** awaiting finalisation.

59. As an example of collaborative success, Operation ARKSTONE is an ongoing AFP-led operation, facilitated through the JACETs in conjunction with New South Wales Police, Western Australia Police and US Homeland Security Investigations. Following information provided by the United States' National Centre for Missing and Exploited Children (NCMEC) to the ACCCE for triage and evaluation, the operation commenced by targeting an alleged online network of offenders producing and sharing child abuse material.

60. Below is a case study of one offender identified through Operation ARKSTONE:

Case Study:

A part of Operation ARKSTONE, the AFP uncovered the online Australian network of alleged child sex offenders after the arrest of a 30 year-old Wyong man in February 2020.

Upon examination of the man's seized electronic devices, investigators followed leads and discovered encrypted social media forums and applications where some members were allegedly producing Child Abuse Material (CAM), while others accessed and circulated CAM. The evidence gathered from the initial arrest led to the unravelling of this alleged online network.

By March 2021, one of the original offenders appeared at court to face **196** charges relating to child sexual abuse and bestiality offences. These included the alleged sexual abuse of young children and filming the abuse to share online including multiple counts of sexual intercourse with a child under 10 years. He had originally been charged with

44 offences but as the investigation continued towards the court hearing, officers continued to examine evidence.

Additional charges were laid as more illicit activity was discovered. This reflects the fact that, even at the brief preparation stage of enforcement activity, officers continue to work hard in assembling and analysing evidence to identify potential offences in conjunction with the Commonwealth Director of Public Prosecutions.

61. Operation ARKSTONE is the largest domestic investigation into online child sexual abuse and continues to yield operational success. As at 31 July 2021, legal proceedings have been initiated against **20** offenders, with a total of **1,236** charges and **54** victims identified. In addition, **146** referrals have been sent to international partners.

Northern Territory Child Abuse Taskforce (NT CAT)

62. The NT CAT provides a targeted joint response to identify and respond to reports of sexual abuse and serious harm against children in the Northern Territory. The taskforce is comprised of members from the AFP, Northern Territory Police and Northern Territory Department of Children and Families (Department). As at June 2021, the AFP has **three** members within the taskforce.

63. The majority of NT CAT engagement is conducted in remote Indigenous communities, within isolated locations in the Northern Territory. The NT CAT response work is augmented by prevention initiatives and targeted operations focusing on community engagement, raising awareness and resilience, and high visibility in communities.

64. This joint police and Department approach reduces the victim's exposure to multiple stakeholders. Its success is amplified by close working relationships between the NT CAT and youth groups, community groups, and government and private entities in health and education.

ThinkUKnow

65. *ThinkUKnow* is an evidence-based education program led by the AFP and delivered nationally to prevent online child sexual exploitation and has been delivered nationally since 2010. The program is a partnership between the AFP, Microsoft Australia, Datacom and the Commonwealth Bank of Australia, and is delivered in collaboration with all state and territory police and Neighbourhood Watch Australasia.

66. *ThinkUKnow* aims to support parents, carers and teachers in preventing and managing safety challenges that children and young people may face online. The program was developed to assist children and young people, from kindergarten/prep to year 12, to identify safe or unsafe situations and know when and how to seek help. The content is pro-technology, encourages help seeking behaviours, and addresses topics including self-generated online child exploitation material, online grooming, image-based abuse and sexual extortion.

67. The rapid increase of children online as a result of COVID-19 reinforces the program's importance. In the 2020/2021 financial year, **25** presentations were delivered to an estimated **1,460** parents, carers and teachers across Australia, while **2,226** presentations were delivered to an estimated **198,680** students.

68. In response to COVID-19 and the suspension of face-to-face presentations, the AFP transitioned to online sessions to support parents, carers and teachers through developing teacher toolkits and at home learning activities.

Operation SOTIERA

69. In February 2021, the AFP established Operation SOTERIA to undertake ongoing environmental scanning into the extent of child sexual abuse and online child safety issues in a small sample of remote indigenous communities. The Operation SOTERIA team consists of AFP investigators and intelligence officers, Online Child Safety and the NT CAT.

70. The environmental scan focuses on local perspectives from police, schools, youth organisations, government and non-government organisations, conducting criminal intelligence analysis and landscape mapping, including technology trends. The scan identifies future prevention and engagement opportunities as well as strategic partnership opportunities.

National Child Offender System

71. Administered by the ACIC, the National Child Offender System (NCOS) helps police protect the community by enabling them to uphold child protection legislation in their state and territory by recording and sharing child offender information. This allows police in each state and territory to meet their obligations under respective child protection legislation.

72. The NCOS consists of the Australian National Child Offender Register (ANCOR) and the Managed Person System (MPS). The ANCOR allows authorised police officers to register, case manage and share information about registered persons. It assists police to uphold child protection legislation in their state or territory.

73. The MPS holds information on alleged offenders who are charged but not convicted, or after an offender's reporting obligations have been completed. It supports the Australian Child Protection Offender Reporting scheme, established by legislation in each state and territory. This scheme requires child sex offenders, and other defined categories of serious offenders against children, to keep police informed of their whereabouts and other personal details for a listed period of time after their release into the community. This register is not intended to be punitive in nature, but is implemented to protect the community by allowing police to exercise authority to case manage offenders thereby reducing the likelihood that an offender will reoffend.

Family Law and Children's Rights Conference

74. The AFP is proud to have been a major sponsor of the 8th *Family Law & Children's Rights Conference: World Congress 2021 'Through the Eyes of a Child'*. Originally

due to be held in Singapore in 2020, the conference was hosted virtually in July 2021.

75. The conference is a major international event which focused on family law, processes and the rights of children and youth. The congress connects lawyers, judges, academics, government, non-government associations, psychologists, medical professionals and social scientists with a common interest in the active protection of children and in sharing best practices to promote the rights of children and family law issues.

76. The AFP delivered five sessions as part of the event and covered topics ranging from prevention efforts, collaboration and coordination in the fight against online child sexual exploitation, families effected by online child sexual exploitation and human trafficking. These sessions included international participants representing the International Centre for Missing and Exploited Children, and NCMEC.

Recently passed laws and legislation before parliament

Combatting Child Sexual Exploitation (CCSE) Act 2019

77. The *Combatting Child Sexual Exploitation Legislation Amendment (CCSE) Act 2019* passed Parliament on 17 September 2019. The CCSE amended the Commonwealth *Crimes Act 1914* and *Criminal Code 1995* to protect children from sexual abuse and exploitation by improving the Commonwealth framework of criminal offences relating to child abuse material including the possession of child-like sex dolls, overseas child sexual abuse, forced marriage, failing to report child sexual abuse and failing to protect children from such abuse.

78. Between its introduction in September 2019 and 30 June 2021, the AFP has commenced proceedings under Criminal Code sections *474.22A possessing or controlling child abuse material obtained or accessed using a carriage service* against **213** people and *273A.1 possessing a child-like sex doll* against **six** people.

Crimes Legislation Amendment (Sexual Crimes against Children and Community Protection Measures) Act 2019

79. *The Crimes Legislation Amendment (Sexual Crimes against Children and Community Protection Measures) Act 2019* passed Parliament on 16 June 2020 and amended the *Crimes Act 1914* and *Criminal Code 1995* to address community concerns regarding sentencing and the evolving use of the internet in child sexual abuse. The Bill also inserted a range of aggravated offences for child sexual abuse, new offences relating to 'grooming' and the provision of electronic services to facilitate dealings with child abuse material online.

Crimes Legislation Amendment (Economic Disruption) Regulations 2021

80. The *Crimes Legislation Amendment (Economic Disruption) Regulations* 2021, which came into force on 5 May 2021, amended the *Proceeds of Crime Regulations 2019* to provide that specified offences relating to child sexual abuse, grooming third parties to procure a child for sexual activity, possessing child-like sex dolls, conduct

in relation to child abuse material, failing to report child sexual abuse and failing to prevent child sexual abuse are 'serious offences' for the purposes of seizing proceeds of crime under the *Proceeds of Crime Act 2002*.

81. To date the AFP has not taken proceeds of crime action against any persons under the new offences within the *Crimes Legislation Amendment (Economic Disruption)* Regulations 2021. The Criminal Assets Confiscation Taskforce (CACT) has taken proceeds of crime action in two matters involving child exploitation matters to date.

82. In November 2020, the AFP restrained the Adelaide home of a man accused of ordering and instructing live-distance child abuse that he watched online. This is the **first time** the AFP has restrained the home of an alleged child sex offender, who is not accused of profiting from his crimes but of allegedly using his property to commit serious offences.

83. On 28 January 2021, the suspect was charged with **50** offences connected with suspected child abuse material found on electronic devices located at his residence. The proceeds of crime proceedings remain before the court.

Impact of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020

84. *The Surveillance Legislation Amendment (Identify and Disrupt)* (SLAID) Bill currently before Parliament proposes new powers for the AFP and the ACIC to identify and disrupt serious crime online, including crime on the dark web and the evasion of law enforcement through use of encryption and anonymising technology.

85. The powers in the SLAID Bill will give law enforcement an edge in disrupting and apprehending offenders. The Bill will introduce three new warrant frameworks, each which will provide critical capabilities for combatting child exploitation material being produced and distributed using anonymising technologies and encryption.

86. It is anticipated that the proposed Account Takeover Warrants (ATW) will assist the AFP in locating child abuse victims and assist in charging offenders with the full scope of their suspected abusive conduct. The ability to takeover an offender's account under an ATW and controlled operation will significantly reduce the length of time for some investigations, as it will allow the AFP to assume the account of the offender on the platforms and chat groups they are already a member of, engaging with others within that forum to gather intelligence and evidence. This removes the need for AFP to spend lengthy periods of time creating online profiles and infiltrating online networks of offenders, which can take up to two years and significantly impact on the welfare of officers.

87. Further, the proposed Data Disruption Warrant may provide assistance in denying offenders access to significant volumes of child abuse material on dark web hidden services, and removing heinous exploitation material so it cannot be further shared, therefore removing the ability for continued victimisation.

Gaps in existing framework

88. The AFP and partners require comprehensive powers, resources and expertise to address the adapting methodologies of child sex offenders and protect the community. AFP operational experience has identified a number of instances where existing legislative frameworks can present challenges and impede the ability to progress an investigation.

89. In these instances, the AFP works closely with the Department of Home Affairs and the Attorney-General's Department to consider appropriate legislative reforms to address gaps identified.

Impact of providers 'going dark' and the adoption of end-to-end encryption

90. The wide scale adoption of end-to-end encryption by major service providers for the stated purpose of protection of individual's private information, has a resulting impact on citizens and societies by eroding a digital platform's ability to detect and respond to illegal content and activity, such as child sexual exploitation and abuse. This, in turn, impacts the ability to inform law enforcement of such crimes and impacts the ability to investigate and collect evidence.

91. The move by the major platforms to end-to-end encryption will have a significant impact upon the ability for law enforcement to detect, identify and respond to offending. Between 01 July 2020 and 30 June 2021, the NCMEC referred **21,399** to the AFP following reports from one major provider. Once that provider moves to end-to-end encryption, they will no longer have visibility of the content being shared across their platforms, and therefore will not be able to detect and refer the matters to the NCMEC. This will result in a significant reduction of referrals to the AFP, making detection and prevention of offending significantly harder for law enforcement.

92. The implications of end-to-end encryption was one of the key issues the AFP Commissioner discussed at his National Press Club address on 22 July 2020. Commissioner Kershaw observed the adoption of end-to-end encryption makes it harder for police to catch predators, noting that the AFP is "very worried about when that day comes, while on the other hand, paedophiles are counting down the days because they cannot wait." The adoption of end-to-end encryption on digital platforms allows predators to remain out of the view of law enforcement and allows their continued offending.

93. The Australian, United Kingdom and United States Governments have publically recognised the need for law enforcement to access information they require to safeguard the public, investigate crimes and prevent future criminal activity.

National Child Offender System

94. Though administered by the ACIC, ACIC access to information and data within the NCOS does not extend to intelligence or investigatory purposes. This significantly limits the Commonwealth government's ability to develop a coordinated national intelligence picture and potential linkages between contact and online child sex

offending. It further limits the ACIC's ability to share relevant information and strategic insights with the AFP and other law enforcement partners.

95. It is anticipated that extending ACIC access to the NCOS would facilitate data analysis and matching against its criminal intelligence and national policing information holdings to:

    - Enhance AFP and partners tactical and strategic targeting of child abuse activities, including by assessing known persons of interest, identifying high priority offenders, refining the profiles and offending patterns of these individuals, and enabling the effective allocation or resources to maximise disruption opportunities.
    - Generate additional insights about the child sexual abuse threat landscape, enabling the AFP, ACCCE and other partners to map, monitor and profile changes.
    - Provide greater visibility to appropriate agencies undertaking prevention and interdiction activities, including national statistics about the number of registers child sex offenders in the NCOS and how these individuals are distributed across Australia.

96. Further, in the event the ACIC was able to leverage their specialist powers and tools, including coercive examinations and human source capabilities, this information could benefit the Commonwealth in developing and disseminating strategic intelligence and break-through understandings of the methodologies, planning and motivations of child sex offender syndicates. ACIC Board approval is required for any expansion of access to NCOS.

Section 3LA

97. Section 3LA of the *Crimes Act 1914* enables the AFP to apply to a magistrate for an order requiring the provision of information or assistance necessary to access data held in, or accessible from, a computer or data storage device.

98. Recent operational experience, including in the child protection space, has demonstrated that although there is a penalty attached to this offence to encourage compliance, this does not always provide sufficient incentive for a person under investigation to comply. In the AFP's experience, persons under investigation for child exploitation offences are often more willing to accept the potential ten year imprisonment offence for failure to comply with a 3LA order, rather than provide access to the device that has evidence of serious offending as these incur more significant penalties.

99. This willingness to accept a penalty rather than complying with 3LA orders creates a significant gap for the AFP, as we are not only unable to gather evidence as to the full scope of that offenders criminality, but it also prevents us gathering essential intelligence on other offenders they are communicating with. The increase in penalty for non-compliance with these orders from 2 years to 10 years in December 2018 did not result in a significant shift in the level of compliance. Broader consideration

of options could be considered, including possible presumption against bail, to ensure that orders are complied with.

Cryptocurrency

100. The increasing use of cryptocurrency as method of payment for child exploitation offenders has presented difficulties for the AFP. Though the AFP has limited abilities to seize or restrain cryptocurrencies, these powers first require identification of the private key or seed phrase that provides access or compliance from the person of interest to facilitate access.

101. Where access has not been possible, or an offender refused to comply with a section 3LA order, the AFP has limited further recourse, and suspects and other parties retain the ability to dissipate the funds upon notification of law enforcement interest.

Proceeds of Crime Act 2002

102. In 2020, the AFP Commissioner set a new strategy for the AFP-led Criminal Assets Confiscation Taskforce to actively investigate whether the assets of child sex offenders can be confiscated. It is anticipated that, as the AFP increasingly targets assets connected with the commission of child exploitation offences (see example at paragraph 82-83 above), suspects will start to structure their offending to avoid forfeiture of their property. For example, a suspect may commit their offending in a rented property instead of a property that they own to prevent their own property from becoming the instrument of their offending.

103. It is important that frameworks adapt to address this criminality, noting that the privacy afforded by a property facilitates the commission and concealment of offending, even though the property may not necessarily need to be altered or adapted for its use in the offending.

Controlled operations

104. The existing controlled operations legislation was built for short-term activities, and was established prior to the emergence of the dark web as a primary facilitator for child exploitation. The covert infiltration of sophisticated dark web criminal syndicates requires long term strategies that require extensive resources and are conducted under the auspices of a major controlled operation.

105. The current legislation limits each authority period to three months, covering a maximum period of 24 months with extensions from the Administrative Appeals Tribunal. This is not reflective of the operational reality associated with progressing long-term operations investigating significant offending. At the 24 month period, the AFP is required to close the original controlled operation prior to gaining approval for a new controlled operation and transferring the existing work to the new approval.

106. The requirement for quarterly extension applications increases the administrative burden on the investigators, with significant supporting material required to gain an extension. A longer initial period for controlled operations, combined with greater extension period would better meet the needs for the type of long and protracted investigations conducted in the child exploitation space.

Conclusion

107. The exploitation of children is a borderless crime that is constantly evolving to evade law enforcement attention and action. The offenders exploiting those vulnerable in our community are highly adaptable and employ technological advancements as they emerge.

108. To address this ever evolving threat, the AFP and partners must work together at local, national and international levels to maintain an ability to coordinate a full suite of expertise, resources and technology to swiftly combat these threats and protect the community.

109. Wherever possible, Australian authorities will pursue, arrest and prosecute Australian-based individuals involved in child exploitation to the fullest extent of the law.

Australian Government

Attorney-General's Department

8 November 2022

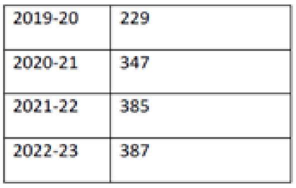
Committee Secretary
Parliamentary Joint Committee on Law Enforcement
le.committee@aph.gov.au

Dear Committee Secretary

Revised Attorney-General's Department's submission to the Inquiry into law enforcement capabilities in relation to child exploitation

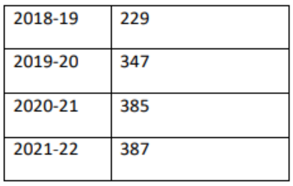
Upon additional quality assurance review of the Attorney-General's Department's submission to the Inquiry into law enforcement capabilities in relation to child exploitation, an error in the financial year timeframes table on page 4 of the submission was identified.

The original submission contains the table below:



2019-20	229
2020-21	347
2021-22	385
2022-23	387

The correct timeframes have been amended in the following table. The correct table is in the attached updated version of the submission.



2018-19	229
2019-20	347
2020-21	385
2021-22	387

I apologise for any inconvenience caused.

Yours sincerely

Tara Inverarity
First Assistant Secretary
International and Security Cooperation Division

Australian Government

Attorney-General's Department

October 2022

Submission to the Inquiry into law enforcement capabilities in relation to child exploitation

Parliamentary Joint Committee on Law Enforcement

Attorney-General's Department

Contents

Overview of Submission

The Department of Home Affairs provided a written submission to the Parliamentary Joint Committee on Law Enforcement (the Inquiry) on 3 September 2021 and appeared at a public hearing on 10 December 2021. A supplementary written submission was submitted to the Inquiry on 12 January 2022 to provide additional context to the statements made by witnesses at the public hearings on 9 and 10 December 2021. The inquiry lapsed in April 2022 when the House of Representatives was dissolved for the general election.

On 3 August 2022 the Committee re-initiated the Inquiry and invited submissions of relevant updates and new evidence. Following the Administrative Arrangements Order of 1 June 2022, responsibility for policy areas that contributed to the first two submissions prepared by the Department of Home Affairs have since transferred to the Attorney-General's Department.

The Attorney-General now has policy responsibilities for the AUS-US Data Access Agreement, and the Budapest Convention on Cybercrime and its Second Additional Protocol. Similarly, the Attorney-General is now responsible for administering the *Telecommunications (Interception and Access) Act 1979* (TIA Act) and relevant offences in the *Criminal Code Act 1995* (Cth), including telecommunications services and computer offences.

This submission provides an update to information previously provided by the Department of Home Affairs relevant to the Inquiry. This submission includes input from portfolio agencies, including the Commonwealth Director of Public Prosecutions (CDPP), Australian Federal Police (AFP) and the Australian Criminal Intelligence Commission (ACIC), Australian Transaction Reports and Analysis Centre (AUSTRAC) and the Australian Institute of Criminology (AIC). This submission should be read alongside the two previous submissions provided by the Department of Home Affairs.

Trends in sentencing, prosecution and offending

Sentencing and prosecution referral

A number of matters have been dealt with under the mandatory minimum sentencing regime, introduced in the *Crimes Legislation Amendment (Sexual Crimes Against Children and Community Protection Measures) Act 2020* which applied to relevant offences committed on or after 23 June 2020.

As at 30 September 2022, 49 offenders were sentenced for offences that had mandatory minimum penalties. 42 of these offenders were subject to the mandatory minimum penalties because they were recidivists, previously convicted of a prescribed child sexual abuse offence and 8 of these offenders were sentenced for the most serious Commonwealth child sex offences which carry mandatory minimum penalties, including for first time offenders.

The number of referrals of matters involving Commonwealth online child sex exploitation offences to the CDPP have increased as follows:

2018-19	229
2019-20	347
2020-21	385
2021-22	387

In the period 1 July 2022 to 30 September 2022, there have been an average of 41 referrals per month of matters involving Commonwealth online child sex exploitation offences. If this trend is maintained, the CDPP will receive almost 500 referrals in the 2022-23 financial year, which would be an increase of 27% in a single year. When compared against data from 2018-19, this referral rate is more than a 100% increase of referrals compared to 5 years ago.

Recent prosecution outcomes

Case Study – Offender identified through payments to known overseas facilitator

AUSTRAC financial intelligence identified a Western Australian man sending funds to a known child sexual exploitation facilitator in the Philippines. Analysis identified payments consistent with the purchase of child abuse material with the offender watching online while victims were exploited in the Philippines. Additional payments were identified being sent to multiple adult facilitators within the Philippines, as well as the use of telecommunication applications to enable the live-distance child abuse to occur. The man procured children as young as seven to engage in sexually explicit acts or be sexually abused on camera, which he watched live from his home.

Following referral to law enforcement, the offender was arrested and was charged with 58 offences including persistent sexual abuse of a child outside Australia, procuring a child to engage in sexual activity outside Australia and soliciting and possessing child abuse material. The Western Australian man pleaded guilty and was sentenced in May 2022 to over 14 years imprisonment after being identified as paying more than $400,000 to sexually abuse children overseas through a home webcam.

Case study – South Australian travelling child sexual offender jailed for 25 years

AUSTRAC financial intelligence identified a 68-year-old South Australian man making payments consistent with the purchase of live-distance child abuse. Additional payments for accommodation and travel in South-East Asia suggested the man was travelling overseas to contact offend against children. The man was arrested when returning to Australia; he had offended against female victims aged between three and nine years of age, with more than 55,000 images and videos of child exploitation material found in his possession.

The man was sentenced in August 2022 to 16 years imprisonment for travelling overseas to sexually abuse children. The offender pleaded guilty to 50 offences, including 41 counts of engaging in sexual activity with a child outside of Australia, using a carriage service to access child exploitation material and possessing child exploitation material. Following AFP investigation, five alleged facilitators of the abuse were arrested in the Philippines and 15 victims were rescued.

Case study – Australian man charged with possessing child like sex doll

A 46-year-old male was sentenced to two years imprisonment after investigators from the Brisbane Joint Anti Child Exploitation Team located six child-like sex dolls during the execution of a search warrant at the man's home. Police also located a laptop at the house which contained child abuse material.

The investigation was launched after AUSTRAC financial intelligence detected financial indicators and purchases of children's clothing including underwear and the Australian Border Force detected a child-like sex doll in a shipment from China on 20 January 2020.

The man was found guilty of two counts of possessing a child-like sex doll or other object that resembles a child (or part of a child) under the age of 18; one count of attempting to possess a child-like sex doll and one count of possessing child exploitation material. The man is the first person in Queensland to be charged and sentenced for this offence, which came into force on 20 September 2019 as part of the *Combatting Child Sexual Exploitation Legislation Amendment Act 2019* (Cth).

Sexual extortion – an emerging online child exploitation trend

Sexual extortion, sometimes called sextortion, is a crime that can involve child victims being coerced by online offenders into sending sexualised images, often through the offender pretending to be another young person. An offender then threatens to on-share the content to others unless their demands are met. These demands can include large amounts of money, gift cards, online gaming credits, more child abuse images, and sexual favours. Despite complying with an offender's demands, the victim may continue to be threatened or extorted. When this happens to someone under the age of 18, it is online child sexual abuse. The coercion and sextortion used by the online offenders causes significant fear and trauma to victims.

Authorities globally are seeing a significant increase in offshore criminal syndicates preying on Australian children, particularly teenage males, coercing them into producing explicit images and then extorting them for money. Despite the increase in reports, it is suspected that the offending is far greater, with many victims not reporting to authorities.

The Attorney-General's Department continues to work closely with law enforcement and prosecutorial agencies to address this trend through awareness raising and reviewing and strengthening legislation to ensure sextortion can be adequately prosecuted.

The AIC has made an updated submission to the current Inquiry outlining recent findings and research related to the emergence of sextortion.

Case Study – Man sentenced for sextortion of young girls

A Sri Lankan national residing in Melbourne was sentenced to jail, after coercing young girls into sending sexually explicit images and videos of themselves and then blackmailing them and distributing the child abuse material to their family and friends, and posting the material to an adult pornography website. The man contacted multiple girls in the United Kingdom, United States of America and Australia, using a fake social media identity. After gaining their trust, the girls sent child abuse material to the man. He then used these images and videos to blackmail them for more content and for money, threatening to share the previously sent material with their friends and family.

AUSTRAC financial intelligence allowed investigators to identify further victims sextorted by this offender. The man was convicted of 25 online child abuse-related offences and sentenced in March 2022 to 13 years and six months' imprisonment with a non-parole period of eight years and six months.

Legislation update

Since the original submission, the *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021* (the SLAID Act) commenced on 4 September 2021. The SLAID Act introduced three new powers for the AFP and the ACIC to identify and disrupt serious online criminal activity. Agencies have commenced using these powers including to target alleged child sexual offenders and drug, firearms and money laundering activities.

Under the *Surveillance Devices Act 2004* and the *Crimes Act 1914*, the AFP Commissioner and the Chief Executive Officer of the ACIC are required to report to the Attorney-General as soon as practicable after the end of each financial year on how agencies have used the powers available under these Acts. This includes details about agencies' use of powers introduced by the SLAID Act. Reports must be tabled in both Houses of Parliament within 15 days of the Attorney-General receiving it. The first reports following the commencement of the new powers will be publicly available in late 2022.

International update

Telecommunications Legislation Amendment (International Production Orders) Act 2021

The *Telecommunications Legislation Amendment (International Production Orders) Act 2021* (IPO Act), was passed by Parliament on 24 June 2021, inserting a new Schedule 1 to the TIA Act. This legislation establishes a legal framework for designating enhanced data access agreements to facilitate law enforcement and national security authority access across borders subject to robust safeguards and criteria.

AUS-US Data Access Agreement

The United States is the largest data controller in terms of communications technologies, services and platforms, which means critical evidence of child exploitation offences is most often located within the United States. On 15 December 2021, the United States and Australia signed the *Agreement between the Government of Australia and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime* (AUS-US Data Access Agreement – previously referred to as the AUS-US CLOUD Act Agreement).

Together with the International Production Order (IPO) framework, the Agreement will reshape Australia's international crime cooperation efforts by expediting the process for obtaining electronic data held in foreign countries. The Agreement achieves this by facilitating direct access to electronic data for investigations of serious crime between the jurisdictions of a foreign country and Australia. The Agreement enables authorities in each country to obtain certain electronic data directly from prescribed communication providers operating in the other's jurisdiction, significantly reducing the time taken to obtain information relevant to the ongoing detection, prevention, investigation and prosecution of serious crime. The Agreement will complement existing international crime cooperation mechanisms, sitting alongside current frameworks such as mutual legal assistance. This provides additional options for Australian agencies to obtain electronic data relating to serious crime from foreign countries.

Australia's use of the Agreement is subject to a range of transparency measures. The IPO Act requires yearly reports to be publicly tabled before the Australian Parliament outlining information on the use of these powers including the number of IPOs obtained, the crime types they related to, the number of arrests, prosecutions and convictions that resulted, and the dissemination of data to Australian law enforcement agencies.

The Agreement is currently subject to consideration by the Joint Standing Committee on Treaties. Once the Australian Parliamentary review process is complete, the Agreement will enter into force upon exchange of diplomatic notes with the US. This will be announced by the Attorney-General by notifiable instrument.

Budapest Convention and Second Additional Protocol

Since the submission provided by the Department of Home Affairs, dated 3 September 2021, there are now over 67 Parties to the Council of Europe Convention on Cybercrime (Budapest Convention) from around the world, with a further 15 countries that are signatories or have been invited to accede.

Australia is an active member of the Cybercrime Convention Committee which represents the State Parties to the Budapest Convention and monitors the effectiveness of the Budapest Convention framework. State Parties to the Convention, including Australia, have the opportunity to shape the development of the committee's position on emerging cybercrime issues. This allows Australia to be involved in meaningfully shaping cybercrime policy to ensure best practice amongst Budapest Convention State Parties. During the period from September 2017 to May 2021, the Cybercrime Convention Committee developed the *Second Additional Protocol on Enhanced Cooperation and Disclosure of Electronic Evidence* to the Budapest Convention. The Protocol opened for signature in May 2022.

The Second Additional Protocol was developed by the State Parties to the Budapest Convention, including Australia, ensuring the Protocol represents the diverse range of legal systems in the international community. The Protocol is anticipated to enhance international cooperation between Parties. As of 28 September 2022, there are 24 signatories to the Protocol.

United Nations Cybercrime Convention

In December 2019, the United Nations General Assembly adopted a resolution to establish an Ad-Hoc Committee process to develop a new United Nations convention on countering the use of information and communications technologies for criminal purposes (sometimes referred to as the UN cybercrime convention). Due to the COVID-19 pandemic, negotiations for this new international treaty were delayed until January 2022. The negotiations are ongoing, with a draft treaty text due to be formulated in early 2023. The Australian delegation is led by the Department of Foreign Affairs and Trade.

During the second negotiating session (30 May – 10 June 2022), the Australian delegation put forward a proposal (publicly available on the Ad Hoc Committee - Home (unodc.org) website) to include provisions criminalising specific online child sexual abuse and exploitation offences in the new convention. This reflects Australia's efforts to raise global standards to combat child sexual abuse and exploitation online. The acceptance of such a proposal as part of the new convention remains outstanding as the text of the proposal has not yet been drafted or finalised.

Five Country Ministerial Forum

To support a holistic response in combatting online child sexual exploitation and abuse, the department is continuing to work with international partners and industry through the Five Country Ministerial [1] to encourage technology companies to voluntarily endorse and implement the *Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse* (the Voluntary Principles)[2]. The department is funded to drive implementation of the Voluntary Principles under the *National Strategy to Prevent and Respond to Child Sexual Abuse.*

The Voluntary Principles were developed in partnership with digital industry (Facebook, Google, Microsoft, Roblox, Snap, TikTok and Twitter), non-government organisations and academia. The Voluntary Principles cover issues ranging from online grooming and livestreaming of child sexual abuse to industry transparency and reporting. Domestic and international governments have partnered with the WeProtect Global Alliance—an international body comprising government, industry and civil society members—to promote the Voluntary Principles globally and drive collective industry action. To date, 16 companies have endorsed the Voluntary Principles, which provide a high-level best practice framework for online platforms and services to combat child sexual abuse and outline ways for companies to take action against online child sexual abuse.

The Five Country Ministerial, through its Digital Industry Engagement Senior Officials Group of which the department is a member, continues to apply pressure on industry to develop baseline voluntary transparency standards to demonstrate how they are tackling child sexual exploitation and abuse on their platforms and services. In June 2022, the Tech Coalition launched their *TRUST: Voluntary Framework for Industry Transparency*[3] which sets out a suggested baseline for industry transparency. The TRUST framework is an important first step in industry-led voluntary frameworks, but does not go far enough in encouraging the sharing of expertise and data.

Vulnerable Populations Community of Practice Working Group

The Vulnerable Populations Community of Practice Working Group (VPCoP) was set up at the end of 2021. It provides a forum for Five Eyes Law Enforcement Group agencies to collaborate on the identification of vulnerable populations being targeted by technology crime enactors involved in child sexual abuse and exploitation. The purpose of the VPCoP is to develop subject matter expert communities of practice focussed on live online child sexual abuse (also known as live streaming of child sexual abuse).

Members of the VPCoP are the ACIC, AFP, ACCCE, US Drug Enforcement Administration, US Federal Bureau of Investigation, US Homeland Security Investigations, UK National Crime Agency, New Zealand Police and Royal Canadian Mounted Police.

[1] The Five Country Ministerial is a forum for the Five Eyes security ministers to meet and discuss opportunities for collaboration on public safety and national security issues.

[2] Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse - WeProtect Global Alliance

[3] Tech Coalition | TRUST: Voluntary Framework for Industry Transparency (technologycoalition.org)

Meetings increase collaboration and develop a common understanding of threats relevant to Five Eyes Law Enforcement Group agencies, exchange information on methodologies and trends and identify and fill intelligence gaps.

United Nations Commission on Crime Prevention and Criminal Justice

Australia contributed to a strong international focus on child sexual exploitation and abuse at the 31st Session of the United Nations Commission on Crime Prevention and Criminal Justice (CCPCJ) held in May 2022. Australia contributed to a strong international focus on tackling child sexual exploitation and abuse across a range of CCPCJ activities.

The AIC moderated a workshop on Improving Criminal Justice Responses to Internet Crimes Against Children, on behalf of the United Nations Crime Prevention and Criminal Justice Programme Network Institutes. The workshop included a presentation showcasing research that explores different ways in which online child sexual abuse is being addressed.

Australia provided support for a UK resolution on protecting children from sexual exploitation and abuse which builds on Australia's 2019 CCPCJ and General Assembly resolutions.

National Strategy to Prevent and Respond to Child Sexual Abuse

The *National Strategy to Prevent and Respond to Child Sexual Abuse 2021-2030* (National Strategy) is a 10-year whole-of-nation framework that provides a coordinated and consistent approach to preventing and better responding to child sexual abuse. The National Office of Child Safety was responsible for designing, and is now responsible for overseeing implementation of the National Strategy. Following the Administrative Arrangements Order of 1 June 2022 the National Office of Child Safety and responsibility for National Strategy oversight has transferred to the Attorney-General’s Department.

Initiatives progressed under the National Strategy

The department has progressed a number of activities funded under the National Strategy, including:

- establishing a Digital Industry Officer position in Washington
- implementing the Indo-Pacific Child Protection Program, and
- driving engagement across government, industry, civil society and academia to raise community and global awareness of law enforcement efforts to target online child sexual exploitation and abuse offenders.

Initiatives aim to stimulate informed debate on digital industry’s crucial role in protecting children from exploitation and abuse online and to support law enforcement and criminal justice policy outcomes. Further information on law enforcement and intelligence related measures can be found under the National Strategy Commonwealth Action Plan and National Action Plan Theme 4.[4]

Screenings of ‘The Children in the Pictures’

The documentary ‘The Children in the Pictures’ follows the investigators and operations initially of the Queensland Police Service Victim Identification Team Taskforce Argos, later located within the Australian Centre to Counter Child Exploitation’s (ACCCE), as they attempt to identify victims of child abuse over a 10-year period.

Over the past 12 months, the department has facilitated international screenings of the documentary in Vienna, New York, London and Ottowa, providing opportunities to engage with like-minded international counterparts. The documentary has highlighted and raised awareness of Australia’s successful law enforcement efforts to counter online child sexual exploitation and abuse.

The department is co-hosting a screening in Washington on 16 November 2022 with the Department of Home Affairs through our Digital Engagement Officer. This event will provide an opportunity to bring in key American senators and decision-makers, and technology industry representatives to view the documentary and facilitate engagement.

Domestically, the department is committed to engaging with industry and non-government partners to screen and utilise the documentary to raise community awareness of the ACCCE and broader law enforcement efforts. Currently, the department is working alongside the non-government organisation, ‘International Justice Mission’ to deliver a screening of the documentary with Australian parliamentarians, senators and government officials at Australia’s Parliament House on 8 November 2022. The event will include a panel discussion on child sexual exploitation and abuse.

Digital Industry Engagement

The department hosts an annual digital industry event which brings together key law enforcement and digital industry representatives to collaborate on initiatives to best support the ACCCE’s operational requirements.

The February 2022 event brought together stakeholders from digital industry, law enforcement, academia, civil society and policy makers to discuss the challenges for law enforcement posed by livestreaming technology as it relates to the distribution of online child sexual abuse. The event provided a valuable forum for building collaborative networks across the many disciplines and organisations that are involved in combatting this crime.

A Washington-based Digital Industry Officer role was established under the National Strategy to build strategic relationships with the technology industry, civil society and academia to combat online child sexual exploitation and abuse. The establishment of the Digital Industry Officer position strengthens the Australian Government’s presence and relationships with international counterparts and industry and provides valuable insight on international efforts and initiatives which will inform Australia’s law enforcement response to online child sexual exploitation and abuse.

[4] Theme 4 of the National Strategy is offender prevention and intervention. Measures under this theme strengthen our criminal justice, law enforcement and intelligence responses to child sexual abuse.

Indo-Pacific Child Protection Program

The Indo-Pacific Child Protection Program delivered its inaugural activity in June 2022, training a cohort of Thai prosecutors on prosecuting online child sexual exploitation and abuse offences, using trauma-informed approach to dealing with child victims and witnesses, and using culturally sensitive practices in dealing with vulnerable victims. The training was well received and shown to fill crucial capacity gaps. The department is currently planning the 2022-23 program of activities for the Indo-Pacific Child Protection Program, which is anticipated to include an environmental scan of the Pacific region, and direct assistance and training across the Indo-Pacific region.

Opportunities to enhance responses

Building the evidence base

One of the most critical aspects of developing effective policy, legislative and operational responses to prevent child sexual abuse is a strong evidence base. In response to the rapid growth of online child sexual exploitation, the AIC has invested significant research effort in better understanding and identifying ways to reduce the problem. The updated AIC submission provided to the Inquiry provides a comprehensive summary of the developments in research and data since submissions to the Inquiry last year, specifically in relation to use of end-to-end encryption by offenders, the link between online and offline sexual offending, sextortion and the role of technology companies in protecting children from harm.

National Child Safety Research Agenda

Recommendation 6.3 of the Final Report of the *Royal Commission into Institutional Responses to Child Sexual Abuse* identified significant gaps in data on the prevalence, nature, extent and impact of child sexual abuse in Australia, and recommended that research be used to build the evidence base.

In response to this recommendation, the National Office for Child Safety is leading the development and delivery of a National Child Safety Research Agenda (CSRA). The CSRA is First National Action Plan Measure 23 of the National Strategy, designed to coordinate and drive national research on child sexual abuse by:

- building evidence on trends and changes in relation to the risk, extent and impact of child sexual abuse victimisation in Australia and offending in Australia and by Australians, for example the link between accessing online child sexual abuse material and contact offending
- assessing the effectiveness of programs, for example legislative tools and law enforcement tactics, that aim to prevent and respond to child sexual abuse
- guiding the development and improvement of new program, legislative and operational reforms, including identifying areas for action under future National Strategy action plans
- linking government and non-government stakeholders with researchers, particularly in areas where research is required to target rapidly evolving trends in offending
- providing incentives for researchers to undertake work aligned with CSRA outcomes.

The National Office for Child Safety is conducting initial consultation and scoping activities this year and throughout 2023, and plans to publish the CSRA in late-2023. As part of these scoping activities, the National

Office for Child Safety will map existing research and identify gaps and limitations in the child safety evidence base, with a particular focus on child sexual abuse. This will inform the nature and prioritisation of future research and the CSRA's research streams.

Throughout CSRA development and delivery, the National Office for Child Safety will work with key stakeholders, including governments, researchers and law enforcement agencies, to identify emerging research needs and coordinate CSRA-aligned research.

Continued need for information and intelligence sharing

The ACIC and AUSTRAC have identified that access to the National Child Offender System remains a significant need. As outlined in the earlier submissions to the Inquiry, access to National Child Offender System would enable the ACIC to undertake data analysis and matching against criminal intelligence and national policing information holdings. Additionally, AUSTRAC's growing role in combatting child sexual exploitation, evidenced by the case studies outlined in this submission, would be further enhanced by access to the National Child Offender System. AUSTRAC's ability to detect child abuse by matching suspicious financial payments with offending, would prioritise actionable intelligence and allow law enforcement to monitor financial activity of registered offenders.

Equally, direct access to the ACIC-managed National Police Record System database would enhance AUSTRAC's capacity to efficiently respond to high priority detection and disruption of child sexual exploitation activities.

Expanding the ACIC and AUSTRAC to access the National Child Offender System would require reforms to relevant State and Territory legislation. Enabling AUSTRAC access to the National Police Record System would require amendments to the Australian Crime Commission Regulations 2018, to make AUSTRAC a prescribed body.

Australian Government
National Office for Child Safety

Submission to the Parliamentary Joint Committee on Law Enforcement

Inquiry into law enforcement capabilities in relation to child exploitation

Our work

About the National Office for Child Safety

The National Office of Child Safety (National Office) was established on 1 July 2018 in response to the Final Report of the Royal Commission into Institutional Responses to Child Sexual Abuse (Royal Commission). The National Office provides national leadership to deliver policies and strategies that enhance children's safety and reduce future harm, with a particular focus on child sexual abuse[1]. This includes leading or co-leading the implementation of 34 Royal Commission recommendations and working across governments and sectors to support the implementation of child safety policies.

As the inquiry's objectives relate mainly to the Home Affairs Portfolio, this submission focuses on where the National Office's national policy leadership role intersects with the inquiry's Terms of Reference.

National Strategy to Prevent and Respond to Child Sexual Abuse

The National Office is responsible for the design, implementation and oversight of Australia's forthcoming *National Strategy to Prevent and Respond to Child Sexual Abuse 2021-2030* (National Strategy). The National Strategy is a key Royal Commission recommendation.

The National Strategy is a 10 year, whole-of-nation framework to establish a coordinated and consistent approach to prevent and better respond to child sexual abuse in all settings, including within families, by other people the child or young person knows or does not know, in organisations, and online. Initially, the National Strategy will be driven by two action plans, both spanning 2021-2024:

- the First National Action Plan will focus on initiatives to be delivered jointly by the Australian Government and state and territory governments
- the First Commonwealth Action Plan will focus on measures to be delivered by the Australian Government.

It is likely these will be followed by two sets of three year action plans (2025-2027 and 2028-2030 respectively) to cover the National Strategy's full 10-year lifespan.

The National Strategy has five themes:

- Theme 1: Awareness raising, education and building child safe cultures
- Theme 2: Supporting and empowering victims and survivors
- Theme 3: Enhancing national approaches to children with harmful sexual behaviours
- Theme 4: Offender prevention and intervention
- Theme 5: Improving the evidence base

Themes 1, 4 and 5 are particularly relevant to the inquiry's Terms of Reference.

The National Strategy will be a truly whole-of-nation response to child sexual abuse. It was developed in consultation with governments, non-government organisations, academics, victims and survivors, Aboriginal and Torres Strait Islander peoples, and people with disability.

In Budget 2021-22, the Australian Government announced $146 million over four years for the first phase of the National Strategy. Additional measures and funding will accompany the full National Strategy's release later in 2021. The National Strategy will include a strong monitoring and evaluation framework to assess how well its measures achieve the National Strategy's vision, objective and values.

[1] This submission uses 'child sexual abuse' to refer to any act that exposes a child or young person to, or involves them in, sexual activities that they do not understand; they do not or cannot consent to; are not accepted by the community; and are unlawful. This definition includes grooming behaviours, contact/physical abuse, and conduct involving child abuse material. In line with the Luxembourg Terminology Guidelines, this definition captures a more expansive range of behaviours than the term 'child exploitation'.

Measures of relevance to the Terms of Reference

Funding law enforcement and prosecutorial agencies

To keep pace with the increasing scale and complexity of Commonwealth child sexual abuse cases, including where offences are committed online, the National Strategy includes:

- $59.9. million worth of initiatives to be delivered by the Australian Federal Police to combat child sexual abuse, including an additional $35.4 million for new frontline operational activities
- $13.9 million to bolster the capabilities of AUSTRAC, the Australian Institute of Criminology, the Australian Border Force, the Australian Criminal Intelligence Commission, and the Department of Home Affairs to equip intelligence, research and border protection agencies to disrupt the cash flow behind child sexual abuse, prevent and disrupt livestreamed child sexual abuse, intercept material and offenders at the border, and enhance our ability to identify offenders within the community
- $24.1 million to strengthen the Commonwealth's capacity to prosecute child sexual abuse cases.

Recognising online child sexual abuse as a priority area

The National Strategy will oversee development of the capabilities, partnerships and strategic insights needed to respond to all forms of online child sexual abuse. Under the National Strategy, the Australian Government will engage key stakeholders to prevent and raise awareness of harmful behaviours online through:

- providing $3.0 million to the Office of the eSafety Commissioner to deliver targeted online education programs to support parents and families to prevent online harms to children
- providing $2.95 million to help the Department of Home Affairs build relationships with the digital industry to drive a coordinated and collaborative charge against offenders' exploitation of online platforms to commit child sexual abuse-related crimes.

Enhancing our understanding of the link between accessing online child abuse material and contact offending

The National Strategy will address gaps in research and data relating to child sexual abuse. This work will enhance law enforcement, intelligence and research agencies' ability to identify offenders within the community, including those engaging in technology-facilitated abuse overseas, and gain insight into offending trajectories.

The Australian Government has already separately funded the first wave of the Australian Child Maltreatment Study (ACMS), which aims to determine the prevalence of all forms of child maltreatment (including sexual abuse) in Australia. The ACMS includes questions on the incidence, context and disclosure of online child sexual abuse, and its co-occurrence with other forms of child maltreatment. The ACMS commenced in January 2019, with preliminary results expected in late-2022 and final results in 2023.

Integrating victim-survivor perspectives to our criminal justice response

Victims and survivors of child sexual abuse face many barriers to disclosing their experiences. Their needs must inform policy design and service delivery. National Strategy measures will be designed using trauma-informed approaches, including where law enforcement and criminal justice outcomes are concerned. Specific measures concerning victims and survivors will be released with the full National Strategy in late 2021.

Australian Government
Australian Institute of Criminology

AIC reports

Inquiry into Law Enforcement Capabilities in Relation to Child Exploitation

Submission to the Parliamentary Joint Committee on Law Enforcement by the Australian Institute of Criminology

Table of contents

Introduction

Thank you for the opportunity to provide a submission to the Parliamentary Joint Committee on Law Enforcement (PJCLE) inquiry into Law Enforcement Capabilities in Relation to Child Exploitation.

The Australian Institute of Criminology (AIC) has a strong history of producing empirical research into child sexual abuse (CSA) and child exploitation. In 2020 the AIC formed the Online Sexual Exploitation of Children Research Program. The Program aims to produce research that helps to understand, prevent, and disrupt child sexual abuse and online sexual exploitation.

This Submission addresses the following point in the Terms of Reference of the inquiry: *'f. Considering the link between accessing online child abuse material and contact offending, and the current state of research into and understanding of that link.'*

Background

Sexual offending against children is a complex and harmful crime that results in ongoing trauma and lifelong adverse consequences for child victims (Cashmore & Shackel 2013). In addition, the viewing, sharing and production of child sexual abuse material (CSAM; also known as child pornography and child exploitation material) is a borderless crime that is flourishing with ongoing advances in technology in the online environment, including internet sites and platforms. According to the Virtual Global Taskforce (2019), police globally struggle to detect CSAM offenders due to the dark web/net and enhanced encryption and anonymisation technologies.

There is evidence that sharing of CSAM on the internet is growing. Bursztein et al. (2019) analysed data from the National Center for Missing and Exploited Children (NCMEC) in the United States (US). Organisations and members of the public can report discovery of CSAM to NCMEC via the CyberTipline and one report can contain from one to hundreds of images/videos. Bursztein and colleagues found that NCMEC received 9.6 million reports of CSAM in 2017 alone, compared with approximately 10,000 reports per year when NCMEC first began recording this information in 1998. They also found that sharing of sexually abusive videos of children dramatically increased from under 1000 video reports per month in 2013 to over 2 million video reports per month in 2017. There was a 379 percent increase in CSAM video reports in 2017 compared to 2016 (Bursztein et al. 2019). There is also evidence of an increase in CSAM production, distribution and viewing since the start of the COVID-19 pandemic. For example, Europol (2020) observed an increase in the sharing of CSAM online, likely due to more offenders and potential victims being at home and online. Indeed, reports of CSAM to NCMEC increased by 28 percent in 2020 at least partly due to COVID-19.

Further, CSAM offending is an evolving crime, with a recent trend towards more harmful and financially motivated methods of exploitation such as live streaming of child sexual abuse (Brown, Napier & Smith 2020; IWF 2018). Because law enforcement often have to investigate sexual offenders who engage in both online and offline (contact) offences, it is important to examine the evidence on how these two offence types are linked.

Are CSAM offenders different to contact sexual offenders?

Firstly, an important question to ask is whether CSAM offenders are different to contact sexual offenders. Babchishin, Hanson and VanZuylen (2015) conducted a meta-analysis of 30 studies produced between 2003 and 2013 from the US, Canada and the UK. Most samples in the studies were selected based on official charges or convictions (94% of CSAM offenders, 91% of contact sexual offenders and 81% of mixed offenders). A minority of studies used self-report or other sources such as accusations (23% of CSAM offenders, 17% of contact sexual offenders and 38% of mixed offenders). The study compared CSAM-only offenders with contact offenders against children and ‘dual offenders’ (those who committed both CSAM and contact offences). They found that CSAM-only offenders differed significantly from contact sexual offenders and dual offenders on a range of characteristics, particularly regarding access to children, sexual deviance and antisocial traits.

Contact offenders were more likely than CSAM-only offenders to have:

- access to children;
- emotional identification with children;
- cognitive distortions (eg ‘children are sexual beings’);
- victim empathy deficits;
- a detached approach to romantic relationships;
- a greater number of prior offences;
- higher scores on measures of antisociality;
- greater problems with supervision;
- indicators of a severe mental illness; and
- childhood difficulties and abuse.

CSAM-only offenders, on the other hand, were more likely than contact offenders to:

- be younger;
- have a higher income and higher education;
- have greater sexual deviancy;
- have problems with sexual preoccupation and sexual self-regulation;
- have greater barriers to contact offending (eg less cognitive distortions).

The study also compared CSAM-only offenders with dual (CSAM and contact) offenders. Dual offenders were more likely than CSAM-only to have:

- access to children;
- a sexual interest in children;
- prior violent offences;
- substance abuse problems; and
- sexual regulation problems.

Dual offenders were also more likely to engage in low commitment sex (eg frequent partners) and report childhood difficulties. However, CSAM-only offenders were more likely than dual offenders to participate in paedophilic social networks or to have other negative social influences.

In another study, Henshaw, Ogloff & Clough (2018) linked data from corrections agencies with policing and mental health records in Victoria, Australia. They compared CSAM offenders (n=456) with contact sexual offenders against children (n=493) and dual offenders (n=256). They found that CSAM-only offenders differed significantly to contact sexual offenders on eight of ten key characteristics measured. Contact offenders were more likely than CSAM-only offenders to have committed a higher number of sexual offences, have offending versatility, have a history of physical violence and intermediate violence (fear/intimidation) and have committed only sexual-related offences. In contrast, CSAM-only offenders were more likely than contact offenders to be of Australian ethnicity, have a higher education and have a paraphilia diagnosis (sexual deviance). Dual offenders (CSAM and contact offending) were found to be a high-risk group with high levels of antisociality and sexual deviance, and thus a greater need for treatment. Thus, there is evidence that CSAM-only offenders differ from contact sexual offenders/dual offenders on a range of characteristics.

A recent systematic review of reoffending by child sexual offenders, conducted by the AIC and focusing on studies published since 2010, found mixed results in studies that compared CSAM offenders with contact child sexual offenders (Dowling et al 2021). Three studies found no difference (Aebi et al. 2014; Jung et al. 2013; Lussier, Deslauriers-Varin & Râtel 2010), while two studies found that contact offenders were more likely to reoffend generally and sexually than CSAM offenders (Laajasalo et al. 2020; Seto & Eke 2015). These studies also found:

- dual offenders were more likely to sexually reoffend than CSAM offenders (Eke, Helmus & Seto 2019; Elliott et al. 2019; Goller et al. 2016; Soldino, Carbonell-Vayá & Seigfried-Spellar 2019); and
- producers of CSAM and those who participated in CSAM networks were more likely to sexually reoffend than other CSAM offenders (Krone et al. 2017).

What proportion of CSAM offenders commit contact sexual offences?

A second important question to ask is how many CSAM offenders also commit contact sexual offences. Seto, Hanson & Babchishin (2011) conducted a meta-analysis of 24 studies based on arrest and conviction figures of online sexual offenders. They found that one in eight (12%) online sexual offenders (CSAM and online grooming offenders) had a *previous* contact sexual offence conviction at time of their online offence.

Where *reoffending* is concerned, an AIC literature review that examined the profile of CSAM offenders found that, up to three percent of CSAM offenders subsequently committed a contact sexual offence, and between 1.6 percent and seven percent committed a further CSAM offence that resulted in criminal justice action (Brown & Bricknell 2018).

Re-analysis of systematic review data gathered by Dowling et al. (2021) was undertaken for this submission. It found that, across 16 studies that examined reoffending by CSAM offenders, between 0.2 percent and 7.5 percent were convicted for a contact sexual offence within 10 years.

In their review of the relationship between CSAM and contact sexual offences for the Royal Commission into Institutional Responses to Child Sexual Abuse, Pritchard and Spironavic (2014) concluded that CSAM-only offenders were at low risk of committing contact sexual offences. However, they also recognised limitations of relying on criminal justice measures.

Self-reported contact sexual offences by CSAM offenders tend to be higher. In the US, Bourke et al. (2015) described how the tactical use of polygraph procedures with a sample of 127 suspects with no prior history of contact child sexual offending resulted in over half disclosing prior offending of this kind (compared with only five percent prior to the polygraph procedure). Seto, Hanson & Babchishin (2011) examined six studies based on self-reports from individuals, finding that 55 percent of online sexual offenders admitted to previously committing a contact sexual offence against a child. This suggests that contact sexual offending by CSAM offenders may be higher than typically acknowledged.

CSAM is a complex crime that is constantly evolving

Most CSAM offending remains undetected

The empirical studies published thus far are largely based on individuals who have been detected for their sexual offences. Yet, the Australian Bureau of Statistics Crime Victimisation Survey finds that only 30 percent of sexual assault victims in Australia report their abuse to police (ABS 2020). According to the Virtual Global Taskforce, 'child sex offenders are finding new ways to perpetuate their crimes online while also making it increasingly more difficult for law enforcement to detect and identify them' (Virtual Global Taskforce 2019: 27).

Further, Hirschtritt, Tucker & Binder (2019) noted a lack of longitudinal research examining whether CSAM offenders progress to contact sexual offending. Therefore, it is likely that a large proportion of CSAM offending remains undetected and under-researched.

CSAM offenders are encouraged by others online to sexually abuse children

CSAM is constantly evolving. In 2019, media outlets reported that the United Kingdom's (UK) National Crime Agency took down a dark web site containing 250,000 videos of children being sexually abused (Voreacos 2019). This resulted in 337 arrests of site users in 11 different countries. It was revealed that users were incentivised to upload their own material of children being abused by receiving 'points' that they could then use to download more material. Forty-five percent of the abusive videos were new to authorities, according to NCMEC (Voreacos 2019).

Similarly, in a recent study, Woodhams et al. (2021) analysed forum posts and private emails/messages of 53 individuals suspected by police of committing CSA and CSAM offences. The individuals conversed with likeminded persons on dark web forums about sexually abusing children or viewing and sharing CSAM. Two conversation topics among these individuals were advice on how to find and approach children to sexually abuse them and how to avoid detection in online and offline sexual offending. Examples such as these suggest that some CSAM viewers can be encouraged by likeminded individuals online to sexually abuse children in person, for the purpose of producing and distributing 'new material'. An analysis of CSA offenders investigated by the Australian Federal Police found that those who engaged in networking with other offenders were significantly more likely to engage in contact sexual offending than those not involved in networks (41% vs 9%) (Krone & Smith 2017).

Online grooming leading to contact sexual abuse

There are also cases in which CSAM content producers will trawl social media sites and chatrooms to find children and young people in order to groom them into supplying sexually explicit images to the perpetrators. Self-created CSAM may be used by online groomers for a range of coercive practices, with threats made by perpetrators including posting the sexual image of the victim online, sending or showing the image to a friend or acquaintance, sending the sexual image to the victim's family, tagging or including the victim's name with a posted image, creating fake accounts of sexual images of the victim, or posting other personal information about the victim along with the image (Wolak et al. 2018). As an indication of the scale of self-created CSAM, the Internet Watch Foundation reported that it dealt with 68,000 cases of 'self-generated' child sexual abuse in 2020. This represented a 77 percent increase on the previous year (Tidy 2021).

Online grooming can also lead to contact sexual abuse as a result of coercing a child to meet with the perpetrator. Indeed, analysis of CyberTipline reports associated with sexual coercion and extortion received by NCMEC estimated that approximately five percent of cases were motivated by the perpetrator wanting to have sex with the child (Europol 2017).

These cases are different to other cases of CSAM reported here in that they represent CSAM *producers* rather than CSAM *consumers*, but they nonetheless show a link between CSAM and contact sexual offending.

Live streaming of child sexual abuse

Live streaming of child sexual abuse (CSA live streaming) is a hybrid form of online child exploitation as it involves the real-time sexual abuse of a child by a third-party, often directed by a live streaming consumer from a distance. Offenders do this often in exchange for money and specify the type of abuse they wish to see (Açar 2017; Europol 2019; Napier, Teunissen & Boxall forthcoming). This crime blurs the line between contact and non-contact sexual offending because offenders direct the abuse of a child in another location. They do this by giving directions to either the facilitator (trafficker) or the victim themselves over online text or video chat (Napier, Teunissen & Boxall forthcoming).

CSA live streaming likely occurs in multiple different countries (Europol 2019). However Southeast Asia, particularly the Philippines, has emerged as a 'hub' for this crime due to its high level of poverty, high-speed internet connection, good English language proficiency and well-established remittance services (ECPAT International 2017). Facilitators in the Philippines can receive an international payment from an offender instantly. Because CSA live streaming offenders communicate and form relationships with victims and facilitators online (unlike with most CSAM viewing), they may be at risk of travelling to offend in person against these children or other children (Europol 2019; Teunissen & Napier forthcoming).

While it is difficult to measure prevalence, anecdotal evidence suggests global demand for CSA live streaming is high. In 2013, four researchers from Terre des Hommes Netherlands posed as pre-pubescent Filipino girls on 19 different online chat forums. Over a 10-week period, 20,172 people from 71 different countries asked the researchers posing as children to perform a webcam sex show (Terre des Hommes 2014). According to International Justice Mission (IJM) who analysed 44 case referrals for online sexual exploitation of children in the Philippines (including CSA live streaming), Australians were the third most common (18%) nationality of offenders (IJM 2020). Brown, Napier & Smith (2020) found that a sample of 256 Australia-based individuals spent $1.3 million AUD to view CSA live streaming in the Philippines over 13 years from 2006 to 2018. This amount was spent over 2,714 separate payments, with the median amount spent on a CSA live streaming transaction being $78 AUD.

In a recent study examining chat logs from CSA live streaming offenders (Napier, Teunissen & Boxall forthcoming), the offending occurred via the open web on popular platforms. Such offences could potentially be traceable by these companies. Yet, the 'end-to-end' encryption proposed on platforms such as Facebook (Hunter 2019) will likely increase the challenges for law enforcement in detecting new and emerging forms of child exploitation. For example, such encryption will prevent police from accessing online chat logs, which are a key form of evidence in the investigation of CSA live streaming. Given that CSA live streaming is another form of contact sexual offending, there is a need for popular online messaging platforms to do more to prevent and disrupt this offending.

More research required

If we are to effectively prevent and disrupt both online and offline sexual offending against children, more research is required that examines the link between these two types of offences. The AIC has received ethical approval to undertake the 'Online survey of sexual offending'. The study will focus on undetected offenders in the community to examine the trajectories of offending. This includes whether there are typical pathways that offenders follow in which their behaviours escalate from less harmful such as deviant pornography and CSAM viewing to more harmful such as CSAM production and contact offending. The AIC is also undertaking a study based on a qualitative analysis of chat logs from people who view CSA live streaming. This study will examine how CSA live streaming intersects with other forms of child sexual abuse, including CSAM and contact offending against children (Teunissen & Napier forthcoming) (see Appendix A for a list of relevant forthcoming AIC research).

Summary

Key issues arising from this review of the evidence are that:

- Most *convicted* CSAM offenders do not go on to commit contact sexual offences against children.
- CSAM offenders who also commit contact sexual offences against children have different characteristics to those who only engage in CSAM.
- Access to children and antisocial characteristics (eg previous arrests) increase the risk of contact sexual offending among CSAM offenders.
- However, this is a constantly evolving crime, and recent evidence suggests:
  - Most CSAM offending likely remains undetected by police;
  - Some CSAM offenders who network with likeminded individuals online are encouraged to sexually abuse children for the purposes of producing and sharing new abusive material;
  - Live streaming of child sexual abuse (CSA live streaming) blurs the line between contact and non-contact sexual offending because offenders direct the abuse of children in another country;
  - Individuals who view CSA live streaming may be at risk of travelling to contact offend against children in vulnerable countries;
  - There is a high global demand for CSA live streaming and due to the ‘live stream’ element, this crime presents challenges for law enforcement in terms of investigation;
  - CSA live streaming offending occurs on the open web on popular platforms; and
  - Increased adoption of end-to-end encryption by popular messaging platforms may increase the challenges in detecting CSA live streaming because police will be unable to access private messages that present as key evidence in this crime.

References

Açar KV 2017. Webcam child prostitution: An exploration of current and futuristic methods of detection. International Journal of Cyber Criminology 11(1): 98–109. https://doi.org/10.5281/zenodo.495775

Aebi M, Plattner B, Ernest M, Kaszynski K & Bessler C 2014. Criminal history and future offending of juveniles convicted of the possession of child pornography. *Sexual Abuse: A Journal of Research and Treatment* 26(4): 375–390. https://doi.org/10.1177/1079063213492344

Australian Bureau of Statistics 2020. Crime Victimisation, Australia, 2018–2019. ABS cat. no. 4530.0. Canberra: ABS. http://www.abs.gov.au/ausstats/abs@.nsf/mf/4530.0

Babchishin KM, Hanson RK & VanZuylen H 2015. Online child pornography offenders are different: A metaanalysis of the characteristics of online and offline sex offenders against children. *Archives of Sexual Behavior* 44(1): 45–66. https://doi.org/10.1007/s10508-014-0270-x

Bourke ML, Frogmeli L, Detar PJ, Sullivan MA, Meyle E & O'Riordan M 2015. The use of tactical polygraph with sex offenders. *Journal of Sexual Aggression* 21(3): 354–367. https://doi.org/10.1080/13552600.2014.886729

Brown R & Bricknell S 2018. What is the profile of child exploitation material offenders? *Trends & issues in crime and criminal justice* no. 564. Canberra: Australian Institute of Criminology. https://www.aic.gov.au/publications/tandi/tandi564

Brown R, Napier S & Smith R 2020. Australians who view live streaming of child sexual abuse: An analysis of financial transactions. *Trends & issues in crime and criminal justice* no. 589. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti04336

Bursztein E, Clarke E, DeLaune M, Elifff DM, Hsu N, Olson L, Shehan J, Thakur M, Thomas K & Bright T 2019. Rethinking the Detection of Child Sexual Abuse Imagery on the Internet. International World Wide Web Conference, San Francisco, 13–17 May: 2601–2607. https://doi.org/10.1145/3308558.3313482

Cashmore J & Shackel R 2013. The long-term effects of child sexual abuse. Child Family Community Australia paper no. 11. Melbourne: Australian Institute of Family Studies. https://aifs.gov.au/cfca/publications/long-term-effects-child-sexual-abuse

Cohen T 2018. Predicting sex offender recidivism: Using the Federal Post-Conviction Risk Assessment instrument to assess the likelihood of recidivism among federal sex offenders. https://doi.org/10.2139/ssrn.2973853

Di Gioia R & Beslay L 2018. *Fighting child sexual abuse: prevention policies for offenders – Inception Report*. Luxembourg: European Union. https://op.europa.eu/en/publication-detail/-/publication/8ecaa7e4-c77f-11e8-9424-01aa75ed71a1/language-en

Dowling C, Boxall H, Pooley K, Long C & Franks C 2021. Patterns and predictors of reoffending among child sexual offenders: A rapid evidence assessment. *Trends & issues in crime and criminal justice* no. tbc. Canberra: Australian Institute of Criminology

Dowling C, Morgan A & Poole K 2021. Reoffending among child sexual offenders. *Trends & issues in crime and criminal justice* no. 628. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti78085

ECPAT International 2017. *Online child sexual exploitation: An analysis of emerging and selected issues.* ECPAT International Journal 12: 1–63. https://www.ecpat.org/wp-content/uploads/2017/04/Journal_No12-ebook.pdf

Eke A, Helmus L & Seto M 2019. A validation study of the Child Pornography Offender Risk Tool (CPORT). *Sexual Abuse* 31(4): 456–476. https://doi.org/10.1177/1079063218762434

Europol 2017. *Online sexual coercion and extortion as a form of crime affecting children: Law enforcement perspective*. The Hague: Europol. https://www.europol.europa.eu/sites/default/files/documents/online_sexual_coercion_and_extortion_as_a_form_of_crime_affecting_children.pdf

Europol 2019. Internet organised crime threat assessment 2019. The Hague: Europol. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019

Europol 2020. Exploiting isolation: Offenders and victims of online child sexual abuse during the COVID-19 pandemic. The Hague: Europol. https://www.europol.europa.eu/publications-documents/exploiting-isolation-offenders-and-victims-of-online-child-sexual-abuse-during-covid-19-pandemic

Elliott IA, Mandeville-Norden R, Rakestrow-Dickens J & Beech AR 2019. Reoffending rates in a UK community sample of individuals with convictions for indecent images of children. *Law and human behavior 43*(4): 369. https://doi.org/10.1037/lhb0000328

Fortin F, Paquette S & Dupont B 2018. From online to offline sexual offending: Episodes and obstacles. *Aggression and Violent Behavior: A Review Journal*, *39*. https://doi.org/10.1016/j.avb.2018.01.003

Goller A, Jones R, Dittman V, Taylor P & Graf M 2016. Criminal recidivism of illegal pornography offenders in the overall population: A national cohort study of 4612 offenders in Switzerland. *Advances in Applied Sociology* 6(2): 48–56. https://doi.org/10.4236/aasoci.2016.62005

Henshaw M, Ogloff JRP & Clough JA 2018. Demographic, mental health, and offending characteristics of online child exploitation material offenders: A comparison with contact-only and dual sexual offenders. *Behavioral Sciences & the Law* 36(2): 198–215. https://doi.org/10.1002/bsl.2337

Henshaw M, Chelsea A, Rajan D, Ogloff J & Clough J 2020. Enhancing evidence-based treatment of child sexual abuse material offenders: The development of the CEM-COPE Program. *Trends & issues in crime and criminal justice* no. 607. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti04787

Henshaw M, Chelsea A, Rajan A, Ogloff J & Clough J 2020. Enhancing evidence-based treatment of child sexual abuse material offenders: The development of the CEM-COPE Program. *Trends & issues in crime and criminal justice* no. 607. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti04787

Hunter F 2019. Encryption can't put tech giants beyond the reach of the law, Minister says. The Sydney Morning Herald. 11 December 11. https://www.smh.com.au/politics/federal/encryption-can-t-put-tech-giants-beyond-the-reach-of-the-law-minister-says-20191211-p53ize.html

Hirschtritt ME, Tucker D & Binder RL 2019. Risk Assessment of Online Child Sexual Exploitation Offenders. *The journal of the American Academy of Psychiatry and the Law 47*(2): 155-164. https://pubmed.ncbi.nlm.nih.gov/30988020/

International Justice Mission (IJM) 2020. Online sexual exploitation of children in the Philippines: Analysis and recommendations for governments, industry and civil society. Summary report. IJM. https://ijmstoragelive.blob.core.windows.net/ijmna/documents/Final_OSEC-Public-Summary_05_20_2020.pdf?bcsi_scan_212274c085d86a74=0&bcsi_scan_filename=Final_OSEC-Public-Summary_05_20_2020.pdf

Internet Watch Foundation (IWF) 2018. Trends in child sexual exploitation: Examining the distribution of captures of live-streamed child sexual abuse. Cambridge, UK: Internet Watch Foundation. https://www.iwf.org.uk/sites/default/files/inline-files/Distribution%20of%20Captures%20of%20Live-streamed%20Child%20Sexual%20Abuse%20FINAL.pdf

Jung S, Ennis L, Stein S, Choy AL & Hook T 2013. Child pornography possessors: Comparisons and contrasts with contact- and non-contact sex offenders. *Journal of Sexual Aggression* 19(3): 295–310. https://doi.org/10.1080/13552600.2012.741267

Krone T & Smith RG 2017. Trajectories in online child sexual exploitation offending in Australia. Trends and issues in crime and criminal justice. No. 524. Canberra: Australian Institute of Criminology. https://www.aic.gov.au/publications/tandi/tandi524

Laajasalo T, Ellonen N, Korkman J, Pakkanen T & Aaltonen O-P 2020. Low recidivism rates of child sex offenders in a Finnish 7-year follow-up. *Nordic Journal of Criminology* 21(1): 103–111. https://doi.org/10.1080/2578983X.2020.1730069

Lussier P, Deslauriers-Varin N & Râtel T 2010. A descriptive profile of high-risk sex offenders under intensive supervision in the province of British Columbia, Canada. *International Journal of Offender Therapy and Comparative Criminology* 54(1): 71–91. https://doi.org/10.1177/0306624x08323236

Middleton D, Mandeville-Norden & Hayes E 2009. Does treatment work with internet sex offenders? Emerging findings from the Internet Sex Offender Treatment Programme (i-SOTP). *Journal of Sexual Aggression*. 15(1): 5–19. https://doi.org/10.1080/13552600802673444

Napier S, Teunissen C & Boxall H forthcoming. Live streaming of child sexual abuse: an analysis of offender chat logs. *Trends & issues in crime and criminal justice*. Canberra: Australian Institute of Criminology

Pritchard J & Spiraonovic C 2014. *Child exploitation material in the context of institutional child sexual abuse*. Report for the Royal Commission into Institutional Responses to Child Sexual Abuse. https://www.childabuseroyalcommission.gov.au/sites/default/files/file-list/Research%20Report%20-%20Child%20Exploitation%20Material%20in%20the%20Context%20of%20Institutional%20Child%20Sexual%20Abuse%20-%20Causes.pdf

Seto M & Eke A 2015. Predicting recidivism among adult male child pornography offenders: Development of the Child Pornography Offender Risk Tool (CPORT). *Law and Human Behaviour* 39(4): 416–429. https://doi.org/10.1037/lhb0000128

Seto MC, Hanson RK, & Babchishin KM 2011. Contact sexual offending by men arrested for child pornography offenses. *Sexual Abuse: A Journal of Research and Treatment* (23): 124-145. https://doi.org/10.1177%2F1079063210369013

Soldino V, Carbonell-Vayá E & Seigfried-Spellar K 2019. Criminological differences between child pornography offenders arrested in Spain. *Child Abuse & Neglect* 98: 104–178. https://doi.org/10.1016/j.chiabu.2019.104178

Terre des Hommes 2014. Webcam child sex tourism: Becoming Sweetie: A novel approach to stopping the global rise of webcam child sex tourism. The Hague: Terre des Hommes. https://www.terredeshommes.org/wp-content/uploads/2013/11/Webcam-child-sex-tourism-terre-des-hommes-NL-nov-2013.pdf

Teunissen C & Napier S forthcoming. How is live streaming of child sexual abuse linked with other forms of child sexual offending? An analysis of offender chat logs. *Trends & issues in crime and criminal justice*. Canberra: Australian Institute of Criminology

Tidy J 2021. *Omegle: Children expose themselves on video chat site.* BBC News, 18 February 2021. https://www.bbc.com/news/technology-56085499

Vedelago C 2020. More than 7.4 million images of child abuse circulating in Victoria. *The Age*, 19 June. https://www.theage.com.au/national/victoria/more-than-7-4-million-images-of-child-abuse-circulating-in-victoria-20200619-p554dy.html

Voreacos D 2019. U.S., South Korea Bust Giant Child Porn Site by Following a Bitcoin Trail. *Bloomberg*, 17 October. https://www.bloomberg.com/news/articles/2019-10-16/giant-child-porn-site-is-busted-as-u-s-follows-bitcoin-trail

Wolak JD, Finkelhor D, Walsh W & Tritman L 2018. Sextortion of minors: Characteristics and dynamics. *Journal of Adolescent Health* 62(1): 72-79. https://doi.org/10.1016/j.jadohealth.2017.08.014

Woodhams J, Kloess JA, Jose B & Hamilton-Giachritsis CE 2021. Characteristics and Behaviors of anonymous users of dark web platforms suspected of child sexual offenses. *Frontiers in Psychology*, 12: 623-668. https://doi.org/10.3389/fpsyg.2021.623668

Sarah Napier is the Manager of the Child Sexual Abuse and Online Exploitation Research Program at the Australian Institute of Criminology
Dr Rick Brown is the Deputy Director of the Australian Institute of Criminology

Appendix A — Relevant current and forthcoming AIC research

Brown R & Bricknell S 2018. What is the profile of child exploitation material offenders? *Trends & issues in crime and criminal justice* no. 564. Canberra: Australian Institute of Criminology. https://www.aic.gov.au/publications/tandi/tandi564

Brown R, Napier S & Smith R 2020. Australians who view live streaming of child sexual abuse: an analysis of financial transactions. *Trends & issues in crime and criminal justice* no. 589. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti04336

Brown R & Shelling J 2019. Exploring the implications of child sex dolls. *Trends & issues in crime and criminal justice* no. 570. Canberra: Australian Institute of Criminology. https://www.aic.gov.au/publications/tandi/tandi570

Cale J Holt T, Leclerc B, Singh S & Drew J 2021. Crime commission processes in child sexual abuse material production and distribution: A systematic review. *Trends & issues in crime and criminal justice* no. 617. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti04893

Cubitt T, Napier S & Brown R 2021. Predicting prolific live streaming of child sexual abuse. *Trends & issues in crime and criminal justice*. Canberra: Australian Institute of Criminology

Dowling C, Boxall H, Pooley K, Long C & Franks C 2021. Patterns and predictors of reoffending among child sexual offenders: A rapid evidence assessment. *Trends & issues in crime and criminal justice* no. tbc. Canberra: Australian Institute of Criminology

Dowling C, Morgan A & Poole K 2021. Reoffending among child sexual offenders. *Trends & issues in crime and criminal justice* no. 628. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti78085

Eggins E, Mazerolle L, Higginson A, Hine L, Walsh K, Sydes M, McEwan J, Hassall G, Roetman S, Wallis R, Williams J 2021. Criminal justice responses to child sexual abuse material offending: A systematic review and evidence and gap map. *Trends & issues in crime and criminal justice* no. 623. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti78023

Henshaw M, Arnold C, Darjee R, Ogloff J, Clough J 2020. Enhancing evidence-based treatment of child sexual abuse material offenders: The development of the CEM-COPE Program. *Trends & issues in crime and criminal justice* no. 607. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti04787

Leclerc B, Drew J, Holt T, Cale J & Sign S 2021. Child sexual abuse material on the darknet: A script analysis of how offenders operate. *Trends & issues in crime and criminal justice* no. 627. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti78160

Lyneham S & Facchini L 2019. Benevolent harm: Orphanages, voluntourism and child sexual exploitation in South-East Asia. *Trends & issues in crime and criminal justice* no. 574. Canberra: Australian Institute of Criminology. https://www.aic.gov.au/publications/tandi/tandi574

McKillop N, Rayment-McHugh S, Smallbone S & Bromham Z 2018. Understanding and preventing the onset of child sexual abuse in adolescence and adulthood. *Trends & issues in crime and criminal justice* no. 554. Canberra: Australian Institute of Criminology. https://www.aic.gov.au/publications/tandi/tandi554

Napier S et al. forthcoming. Examining pathways between non-contact and contact sexual offending: Findings from the 'Online survey of sexual offending'. *Trends & issues in crime and criminal justice*. Canberra: Australian Institute of Criminology

Salter M, Wong WKT, Breckenridge J, Scott Sue, Cooper S & Peleg N 2021. Production and distribution of child sexual abuse material by parental figures. *Trends & issues in crime and criminal justice* no. 616. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti04916

Teunissen C & Napier S forthcoming. How is live streaming of child sexual abuse linked with other forms of child sexual offending? An analysis of offender chat logs. *Trends & issues in crime and criminal justice*. Canberra: Australian Institute of Criminology

Inquiry into Law Enforcement Capabilities in Relation to Child Exploitation

Submission to the Parliamentary Joint Committee on Law Enforcement by the Australian Institute of Criminology

Contents

Introduction

Thank you for the opportunity to provide a submission to the Parliamentary Joint Committee on Law Enforcement inquiry into Law Enforcement Capabilities in Relation to Child Exploitation.

The Australian Institute of Criminology (AIC) has a strong history of producing empirical research into child sexual abuse (CSA). In 2020 the AIC formed the Online Sexual Exploitation of Children Research Program. The program aims to produce research that helps to understand, prevent and disrupt child sexual abuse and online sexual exploitation.

This submission addresses the following points in the terms of reference of the inquiry:

> d. considering the use by offenders of encryption, encryption devices and anonymising technologies, and Remote Access Trojans to facilitate their criminality, along with the resources of law enforcement to address their use;
>
> e. considering the role technology providers have in assisting law enforcement agencies to combat child exploitation, including but not limited to the policies of social media providers and the classification of material on streaming services; and
>
> f. Considering the link between accessing online child abuse material and contact offending, and the current state of research into and understanding of that link.

Background

Sexual offending against children is a complex and harmful crime associated with ongoing trauma and lifelong adverse consequences for child victims, including psychiatric disorders, substance abuse, revictimisation and offending in adulthood (Cashmore & Shackel 2013; Hailes et al. 2019; Ogloff et al. 2012). In addition, the viewing, sharing and production of child sexual abuse material (CSAM; also known as child pornography and child exploitation material) is a borderless crime that is flourishing with ongoing advances in technology in the online environment, including internet sites and social media platforms (Teunissen & Napier 2022).

There is evidence that CSAM has proliferated in recent years (Balfe et al. 2015; Bursztein et al. 2019). The National Center for Missing and Exploited Children (NCMEC) in the United States received over 21 million reports of online sexual exploitation (most of which were CSAM) in 2020 alone (NCMEC 2021), increasing to over 29 million in 2021 (NCMEC 2022a). In an analysis of NCMEC data, Bursztein et al. (2019) found that reports of sexually abusive videos of children dramatically increased from under 1,000 video reports per month in 2013 to over two million video reports per month in 2017. This equated to a 379 percent increase in CSAM video reports in 2017 compared with 2016 (Bursztein et al. 2019).

In addition, the problem may have been exacerbated by global events such as the COVID-19 pandemic (Interpol 2020). Europol (2020) observed an increase in the sharing of CSAM online, likely due to more offenders and potential victims being at home and online. Law enforcement agencies struggle to keep up with the staggering number of CSAM reports to investigate (NCMEC 2021; Netclean 2020). According to Netclean (2020), which surveyed 470 law enforcement officers in 39 countries, in 2020 police globally were inundated with CSAM cases. This affected the mental health of officers and meant they could investigate only the most high-risk cases.

Also of concern is that online sexual exploitation of children is an evolving crime, with a recent trend towards more harmful and financially motivated methods of exploitation such as ‘sextortion’ (discussed below; Patchin & Hinduja 2020; Wolak et al. 2018) and live streaming of child sexual abuse (Brown, Napier & Smith 2020; Internet Watch Foundation 2018). Further, the use of end-to-end encryption by communication platforms, while designed for user safety, may present challenges for law enforcement in combatting CSAM offending. It is important to examine the use of encryption by online offenders on social media platforms and the role of tech companies in protecting children from sexual abuse and exploitation.

Lastly, there is often a lack of clarity around the association between offline (contact) and online sexual offences against children. Because law enforcement often investigate sexual offenders who engage in both online and offline offences, it is also important to examine the evidence on how these two offence types are linked.

Are CSAM offenders different to contact sexual offenders?

Firstly, an important question to ask is whether CSAM offenders are different to contact sexual offenders. Babchishin, Hanson and VanZuylen (2015) conducted a meta-analysis of 30 studies produced between 2003 and 2013 from the United States, Canada and the United Kingdom. Most samples in the studies were selected based on official charges or convictions (94% of CSAM offenders, 91% of contact sexual offenders and 81% of mixed offenders). A minority of studies used self-report or other sources such as accusations (23% of CSAM offenders, 17% of contact sexual offenders and 38% of mixed offenders). The study compared CSAM-only offenders with contact offenders against children and 'dual offenders' (those who committed both CSAM and contact offences). They found that CSAM-only offenders differed significantly from contact sexual offenders and dual offenders on a range of characteristics, particularly regarding access to children, sexual deviance and antisocial traits.

Contact offenders were more likely than CSAM-only offenders to have:

- access to children;
- emotional identification with children;
- cognitive distortions (eg a belief that 'children are sexual beings');
- victim empathy deficits;
- a detached approach to romantic relationships;
- a greater number of prior offences;
- higher scores on measures of antisociality;
- greater problems with supervision;
- indicators of a severe mental illness; and
- childhood difficulties and abuse.

CSAM-only offenders, on the other hand, were more likely than contact offenders to:

- be younger;
- have a higher income and higher level of education;
- have greater sexual deviancy;
- have problems with sexual preoccupation and sexual self-regulation; and
- have greater barriers to contact offending (eg less cognitive distortions).

The study also compared CSAM-only offenders with dual (CSAM and contact) offenders. Dual offenders were more likely than CSAM-only offenders to have:

- access to children;
- a sexual interest in children;
- prior violent offences;
- substance abuse problems; and
- sexual regulation problems.

Dual offenders were also more likely to engage in low-commitment sex (eg many partners) and report childhood difficulties. However, CSAM-only offenders were more likely than dual offenders to participate in paedophilic social networks or to have other negative social influences.

In an Australian study, Henshaw, Ogloff and Clough (2018) linked data from corrections agencies with policing and mental health records in Victoria. They compared 456 CSAM offenders with 493 contact sexual offenders against children and 256 dual offenders. They found that CSAM-only offenders differed significantly to contact sexual offenders on eight out of 10 key characteristics measured. Contact offenders were more likely than CSAM-only offenders to have committed a higher number of sexual offences, have offending versatility, have a history of physical violence and intermediate violence (fear/intimidation) and have committed only sexual offences. In contrast, CSAM-only offenders were more likely than contact offenders to have a higher education and have a paraphilia diagnosis (sexual deviance). Dual offenders (CSAM and contact offending) were found to be a high-risk group with high levels of antisociality and sexual deviance and therefore a greater need for treatment. Thus, there is evidence that CSAM-only offenders differ from contact sexual offenders and dual offenders on a range of characteristics.

A recent systematic review of reoffending by child sexual offenders, conducted by the AIC and focusing on studies published since 2010, found mixed results in studies that compared CSAM offenders with contact child sexual offenders (Dowling et al. 2021). Three studies found no difference (Aebi et al. 2014; Jung et al. 2013; Lussier, Deslauriers-Varin & Râtel 2010), while two studies found that contact offenders were more likely to reoffend generally and sexually than CSAM offenders (Laajasalo et al. 2020; Seto & Eke 2015). These studies also found:

- dual offenders were more likely to sexually reoffend than CSAM offenders (Eke, Helmus & Seto 2019; Elliott et al. 2019; Goller et al. 2016; Soldino, Carbonell-Vayá & Seigfried-Spellar 2019); and
- producers of CSAM and those who participated in CSAM networks were more likely to sexually reoffend than other CSAM offenders (Krone et al. 2017).

What proportion of CSAM offenders commit contact sexual offences?

A second important question to ask is how many CSAM offenders also commit contact sexual offences. Seto, Hanson and Babchishin (2011) conducted a meta-analysis of 24 studies based on arrest and conviction figures of online sexual offenders. They found that one in eight (12%) online sexual offenders (CSAM and online grooming offenders) had a previous conviction for a contact sexual offence at time of their online offence.

Where *reoffending* is concerned, an AIC literature review that examined the profile of CSAM offenders found that up to three percent of CSAM offenders subsequently committed a contact sexual offence, and between 1.6 percent and seven percent committed a further CSAM offence that resulted in criminal justice action (Brown & Bricknell 2018).

Re-analysis of systematic review data gathered by Dowling et al. (2021) was undertaken for this submission. It found that, among the CSAM offenders examined in 16 studies, between 0.2 percent and 7.5 percent were convicted of a contact sexual offence within 10 years.

Similarly, a recent study by Morgan (2022) explored the characteristics of recidivist child sexual assault offenders, victims and incidents, analysing data from four Australian states: New South Wales, Queensland, Victoria and Western Australia. The author explored the characteristics of contact child sexual offences involving an alleged offender who had a prior recorded history of alleged child sexual offences. Morgan found that between four and 17 percent of alleged offenders in the sample had transitioned from non-contact to contact sexual offences, thus supporting Dowling et al. (2021) and indicating that most detected CSAM offenders are not detected for subsequent contact sexual offences.

In their review of the relationship between CSAM and contact sexual offences for the Royal Commission into Institutional Responses to Child Sexual Abuse, Prichard and Spiranovic (2014) concluded that CSAM-only offenders were at low risk of committing contact sexual offences. However, they also recognised the limitations of relying on criminal justice measures. Similarly, Hirschtritt, Tucker and Binder (2019) noted a lack of longitudinal research examining whether CSAM offenders progress to contact sexual offending.

While most research in this area has focused on criminal justice measures of sexual offending (eg arrests or convictions), research on self-reported contact sexual offences by CSAM offenders tends to find higher rates. In the United States, Bourke et al. (2015) described how the tactical use of polygraphs with a sample of 127 suspects with no recorded history of contact child sexual offending resulted in over half disclosing prior offending of this kind (compared with only 5% prior to the polygraph procedure). Seto, Hanson and Babchishin (2011) examined six studies based on self-reports from individuals, finding that 55 percent of online sexual offenders admitted to previously committing a contact sexual offence against a child.

Lastly, Insoll et al. (2022) surveyed 1,546 individuals who searched for CSAM on the darknet, finding that 42 percent of respondents reported seeking direct contact with children through online platforms after viewing CSAM or illegal violent material, and 58 percent reported feeling concerned that viewing of CSAM or illegal violent material could lead to sexual acts against a child or adult. While the study was likely biased towards more serious offenders due to recruitment via the darknet, it nevertheless suggests that contact sexual offending (or attempted offending) by CSAM offenders may be higher than typically reported in much of the research.

CSAM is a complex and constantly evolving crime

How much CSAM offending is detected?

The empirical studies published thus far are largely based on individuals whose sexual offences have been detected. Yet the Australian Bureau of Statistics Crime Victimisation Survey finds that only 30 percent of sexual assault victims in Australia report their abuse to police (ABS 2020). There have been similar findings relating to CSAM offending. A survey of 133 victim-survivors of CSAM offending found only one in four (23%) of the CSAM incidents were reported to the police or a child welfare agency (Gewirtz-Meydan et al. 2018). Therefore, it is possible that a large proportion of CSAM offending remains undetected.

CSAM offenders encourage each other online to sexually abuse children

Another concerning factor to emerge in the online sexual exploitation of children is that these offenders tend to network with and encourage one another to sexually abuse children. In 2019, media outlets reported that the United Kingdom’s National Crime Agency took down a darknet site containing 250,000 videos of children being sexually abused (Voreacos 2019). This resulted in 337 arrests of site users in 11 different countries. It was revealed that users were incentivised to upload their own material of children being abused—for each upload, they received ‘points’ that they could use to download more material. Forty-five percent of the abusive videos were new to authorities, according to NCMEC (Voreacos 2019).

Similarly, in a recent study, Woodhams et al. (2021) analysed forum posts and private emails/messages of 53 individuals suspected by police of committing CSA and CSAM offences. The individuals conversed with like-minded persons on darknet forums about sexually abusing children or viewing and sharing CSAM. Two conversation topics among these individuals were advice on how to find and approach children to sexually abuse and how to avoid detection in online and offline sexual offending. These examples suggest that some CSAM viewers can be encouraged by like-minded individuals online to sexually abuse children in person, for the purpose of producing and distributing new material. An analysis of CSA offenders investigated by the Australian Federal Police found that those who engaged in networking with other offenders were significantly more likely to engage in contact sexual offending than those not involved in networks (41% vs 9%; Krone & Smith 2017).

Online grooming can lead to contact sexual abuse

There are also cases in which CSAM content producers will trawl social media sites and chatrooms to find children and young people in order to groom them into supplying sexually explicit images. Self-created CSAM may be used by online groomers for a range of coercive practices (eg sextortion). For example, perpetrators may threaten to post the sexual image of the victim online, send or show the image to a friend or acquaintance, send the image to the victim's family, tag or include the victim's name with a posted image, create fake accounts using sexual images of the victim, or post other personal information about the victim along with the image (Wolak et al. 2018). According to the NCMEC, 'sextortion' is:

> … a form of child sexual exploitation where children are threatened or blackmailed, most often with the possibility of sharing with the public a nude or sexual images of them, by a person who demands additional sexual content, sexual activity or money from the child. (NCMEC 2022b)

As an indication of the scale of self-created CSAM, the Internet Watch Foundation reported that it dealt with 68,000 cases of 'self-generated' material in 2020. This represented a 77 percent increase on the previous year (Tidy 2021).

Other evidence also suggests that this form of crime is increasing. In a nationally representative survey of 5,568 high school students in the United States aged 12–15 years, approximately five percent reported that they had been the victim of sextortion (Patchin & Hinduja 2020). The NCMEC reported that between 2019 and 2021, the number of reports to their CyberTipline that involved sextortion against children more than doubled (NCMEC 2022b). Similarly, in a media article published in May 2022, the FBI reported that sextortion against children had been increasing and evolving in recent years (Torres-Cortez 2022).

Online grooming and sextortion can also lead to contact sexual abuse, where the perpetrator coerces a child to meet with them. Indeed, analysis of CyberTipline reports associated with sexual coercion and extortion received by NCMEC estimated that approximately five percent of cases were motivated by the perpetrator wanting to have sex with the child (Europol 2017). These cases are different to other cases of CSAM reported here in that they represent CSAM *producers* rather than CSAM *consumers*, but they nonetheless show a link between CSAM and contact sexual offending, particularly when the offender demands to meet the child in person.

Lastly, there is evidence that adults can be groomed online for access to their children. Teunissen et al. (2022) surveyed nearly 10,000 users of mobile dating apps and websites in Australia, finding that 12.4 percent had received at least one request for child sexual exploitation from another mobile dating app user. Requests included asking for photos of children (either the respondent's own children or others they had access to), asking for sexual photos of the children, asking inappropriate questions about the children (eg breast size), asking to meet the children in person before it was appropriate, and offering payment for the children to perform on webcam. This tells us that offenders are now using mobile dating apps to groom adults for child sexual exploitation, and potentially child sexual abuse in person, although the study did not explore this latter aspect in great depth.

Live streaming of child sexual abuse

Live streaming of child sexual abuse (CSA live streaming) is a hybrid form of online child exploitation as it involves the real-time sexual abuse of a child by a third party, often directed by a live streaming consumer from a distance. Offenders pay to watch a child being abused over online video chat, and often specify the type of abuse they wish to see (Açar 2017; Europol 2019; Napier, Teunissen & Boxall 2021). This crime blurs the line between contact and non-contact sexual offending because offenders direct the abuse of a child in another location. They do this by giving directions to either the facilitator (usually the victim's family member) or the victim themselves over online text or video chat (Napier, Teunissen & Boxall 2021).

CSA live streaming likely occurs in multiple different countries (Europol 2019). However, South-East Asia, particularly the Philippines, has emerged as a hub for this crime due to its high level of poverty, high-speed internet connection, English language proficiency and well-established remittance services (ECPAT International 2017). Facilitators in the Philippines can receive an international payment from an offender instantly. Because CSA live streaming offenders (unlike other CSAM offenders) communicate and form relationships with victims and facilitators online, they may be at risk of travelling to offend in person against these children or other children (Europol 2019; Teunissen & Napier forthcoming).

While it is difficult to measure prevalence, anecdotal evidence suggests global demand for CSA live streaming is high. In 2013, four researchers from Terre des Hommes Netherlands posed as pre-pubescent Filipino girls on 19 different online chat forums. Over a 10-week period, 20,172 people from 71 different countries asked the researchers posing as children to perform a webcam sex show (Terre des Hommes 2014). According to International Justice Mission, who analysed 44 case referrals for online sexual exploitation of children in the Philippines (including CSA live streaming), Australians were the third most common (18%) nationality of offenders (International Justice Mission 2020). Brown, Napier and Smith (2020) found that a sample of 256 Australia-based individuals spent A$1.3 million to view CSA live streaming in the Philippines over 13 years from 2006 to 2018. This amount was spent over 2,714 separate payments, with the median amount spent on a CSA live streaming transaction being A$78. Further, in a recent study examining chat logs from CSA live streaming offenders, Teunissen and Napier (forthcoming) found that CSA live streaming offenders sometimes requested to meet children in the Philippines in person either before or after directing and viewing their abuse live over webcam.

Use of encryption by offenders

End-to-end encryption ensures that information on a platform is visible only to the individual or entity who has the ‘key’ to decrypt it (Schiemer 2018), and in almost all cases, this is only the sender and recipient. This is designed to protect sensitive and personal information such as messages and transactions (eSafety Commission 2020), and also to protect users from malicious online activity such as cybercrime (Amnesty International 2016). Data show that apps with security features have more active users (Stevens 2020), which demonstrates the appeal of privacy to the public.

Unfortunately, end-to-end encryption presents significant challenges to law enforcement officers who investigate CSAM offending (Netclean 2019), and limits companies’ ability to prevent, detect and report CSAM occurring on their platforms. For example, online chat logs are a key form of evidence in CSAM investigations. In one such Australian case, the offender used several popular platforms to distribute CSAM he had produced, which involved severe abuse of babies (*Commonwealth Director of Public Prosecutions v CCQ* [2021] QCA 4 (22 January 2021); warning: contains highly graphic details of abuse). In this case the offender’s chat logs were used as evidence to demonstrate the severity of offending that took place. In another case, Meta detected CSAM in a conversation between an Australian man and a Filipino child, leading to the man’s arrest when he travelled to the Philippines (Murdoch 2016). If the platforms used by these offenders had implemented end-to-end encryption at that time, this evidence may not have been available for investigations and the offenders may still be at large.

Currently, four of the companies that send the top 10 number of CSAM reports to NCMEC use end-to-end encryption for private messages on some of their platforms: Meta (used on WhatsApp), Google, Snap and Skype (Teunissen & Napier 2022). WhatsApp has two billion users (WhatsApp 2020)—more than both Facebook Messenger (988 million; Statista 2022a) and Instagram (1 billion; Statista 2022b). However, given its use of end-to-end encryption, CSAM cannot be detected in WhatsApp conversations unless users report it.

Meta plans to implement universal end-to-end encryption on Facebook Messenger and Instagram’s private messages in 2023 (Davis 2021; Kent 2021). These are two of the largest social media platforms in the world. There are concerns that CSAM detection technologies currently used by these platforms (eg PhotoDNA, artificial intelligence tools) will not work in an end-to-end encryption environment as they will be unable to decrypt the content and scan it for CSAM (NCMEC 2019). To our knowledge, Meta has not publicly proposed a strategy to maintain its ability to detect and report CSAM on these platforms once it introduces end-to-end encryption next year. As most CSAM on Facebook Messenger is detected using PhotoDNA and artificial intelligence tools (Facebook nd; Farid 2019), NCMEC has estimated that Meta's implementation of end-to-end encryption across all its major platforms will reduce the number of CSAM reports it receives by more than 50 percent (NCMEC 2019). This does not mean that CSAM offending will be reduced; rather, Meta will no longer be able to detect it.

Role of tech companies

As outlined above, evidence shows that significant amounts of CSAM are detected on popular social media platforms, and distribution of this material occurs at a rate far exceeding that of pre-internet days. Consequently, this problem is beyond the capability of law enforcement to address alone. Therefore, the companies that run these platforms have a responsibility to prevent offending and remove abusive material. The AIC examined transparency reports and other publicly available information from electronic service providers (ESPs; eg Meta; Teunissen & Napier 2022). The 10 ESPs that sent the largest number of CSAM reports to NCMEC in 2020 were identified via the *2021 CyberTipline reports by electronic service providers* (NCMEC 2022a). This study found that the platforms with the highest user bases state that they are actively detecting and removing CSAM (Teunissen & Napier 2022). However, some are less transparent than others about the methods they use to prevent, detect and remove CSAM, omitting key information that is crucial for future best practice in reducing CSAM offending. There was little reliable or detailed information available on definitions of CSAM used and, for some ESPs, the detection and prevention tools used and their effectiveness. Further, the adoption of end-to-end encryption by platforms that detect and remove large amounts of CSAM from their platforms will likely provide a haven for CSAM offenders.

In an earlier study of chat logs from CSA live streaming offenders, Napier, Teunissen and Boxall (2021) found that live streaming of CSA occurred via the open web on popular video chat platforms including Facebook Messenger, Skype and Viber. Similarly, in its 2019 report Netclean found that that Skype was the most common platform used for live streaming of CSA (Netclean 2019). Such offences could potentially be traceable by these companies. However, Teunissen and Napier (2022) found little information available on the methods currently used by ESPs to prevent or detect live streaming of CSA. It is therefore not publicly known whether ESPs currently use, or are developing, such methods.

While most major ESPs are publicly opposed to online sexual exploitation of children and proactively detect and remove CSAM, they are unfortunately still inadvertently facilitating this offending. There are also concerns that these companies are deflecting responsibility for preventing CSAM distribution and focusing on reporting CSAM if they find it (Salter & Hanson 2021). The burgeoning number of CSAM reports from ESPs places a huge burden on law enforcement, who struggle to keep up with the workload (NCMEC 2021; Netclean 2020). There are several measures that tech platforms/ESPs should adopt to help address the problem.

Implications for ESPs

Firstly, every company should be consistent in their reporting of CSAM and transparent about their definitions of CSAM and the specific measures they use to prevent, detect and report it. Providing this detailed information will help enforce best practice standards and assist companies to improve their tools for preventing harm to children.

Secondly, more responsibility should be placed on ESPs to prevent CSAM from being uploaded in the first instance. These platforms should adopt evidence-based methods such as pop-up warning messages, which can deter the viewing or sharing of CSAM and refer individuals to sources of help (Prichard et al. 2022). Deterrence messaging campaigns can also reach large numbers of individuals (Grant et al. 2019). These tools should also be evaluated; Meta currently uses pop-up warning messages to deter child sexual exploitation, yet there is no information publicly available on their impact or effectiveness.

Lastly, ESPs should invest in more innovative technology. Currently, NeuralHash, Apple's proposed technology to scan devices for CSAM, is the only publicly described tool that will detect CSAM in an end-to-end encryption environment. Although Apple has delayed the release of this technology (Wakefield 2021), communication platforms should similarly invest in developing technology to prevent CSAM from being uploaded onto their platforms. This would supplement their current methods of detecting CSAM and removing it from their platforms, and will assist law enforcement with investigations.

Implications for international law reform

The increasing availability of CSAM on major platforms will result in continuing and increased harm to children. Yet debate continues over the importance of protecting children versus protecting the privacy of individuals (Allen 2021). The adoption of end-to-end encryption by more ESPs will likely provide a haven for CSAM offending, rather than preventing it. Further policy discussions are required about how to address the risk that end-to-end encryption will increase the difficulty of detecting, preventing and investigating CSAM offences, taking into account the impact on current and future child victims. These discussions should also consider the development of detection tools that could operate in the end-to-end encryption environment.

Secondly, it would be beneficial for countries globally, including the Five Eyes nations and European nations, to introduce legislation requiring tech platforms to report CSAM consistently and adopt evidence-based detection and prevention measures. Additionally, companies should be consistent and transparent in how they report:

- definitions of CSAM;
- the amount of CSAM detected and removed;
- the number of accounts banned, suspended and/or deleted due to child sexual exploitation;
- details of their methods of detecting and removing CSAM;
- details of their methods of preventing CSAM offending (eg messaging campaigns, warning messages); and
- evaluations of the effectiveness of these methods in detecting and preventing CSAM offending.

Adopting such legislation will help reduce the sexual abuse and online sexual exploitation of children globally.

Summary

Link between online and contact sexual offending

Key issues arising from this review of the evidence are that:

- Most convicted CSAM offenders do not go on to commit contact sexual offences against children.
- CSAM offenders who also commit contact sexual offences against children have different characteristics to those who only engage in CSAM.
- Access to children and antisocial characteristics (eg previous arrests) increase the risk of contact sexual offending among CSAM offenders.
- CSAM is a constantly evolving crime, and recent evidence suggests:
  - – Most CSAM offending may remain undetected by police;
  - – Online grooming and sextortion can lead to contact sexual offending against children;

  - Some CSAM offenders who network with like-minded individuals online are encouraged to sexually abuse children for the purposes of producing and sharing new abusive material;
  - Live streaming of child sexual abuse blurs the line between contact and non-contact sexual offending because offenders direct the abuse of children in another country;
  - Individuals who view CSA live streaming may be at risk of travelling to offend against children in vulnerable countries in person; and
  - There is a high global demand for CSA live streaming, which, because of the 'live stream' element, is difficult for law enforcement to investigate.
- If we are to effectively prevent and disrupt both online and offline sexual offending against children, more research is required that examines the link between these two types of offences.

Encryption used by online offenders

- Increased adoption of end-to-end encryption by popular tech platforms will probably increase the challenges in detecting online sexual exploitation of children because police will be unable to access private messages that form key evidence in these crimes.
- CSA live streaming occurs on popular platforms, some of which use end-to-end encryption, creating further challenges for law enforcement in detecting these offences.
- While many large tech companies (eg Meta) are moving towards the use of end-to-end encryption, most have not publicly announced if and how they will detect, prevent and remove CSAM in such an environment.

The role of tech companies in protecting children from harm

- While most major ESPs are publicly opposed to CSAM offending, they are unfortunately still inadvertently facilitating its distribution.
- It is the responsibility of ESPs to protect children from harm on their platforms. They should do so by:
  - being transparent and consistent in their reporting of CSAM and in their definitions of CSAM and the specific measures they use to prevent, detect and report it;
  - adopting evidence-based methods such as pop-up warning messages and deterrence messaging campaigns, which can deter use of CSAM and refer individuals to sources of help; and
  - developing more innovative technology to detect and prevent CSAM and other forms of child sexual exploitation.
- Further policy discussions are required about how to prevent end-to-end encryption from impeding the detection and investigation of CSAM offences, and about technologies that may assist law enforcement to protect children from harm in this environment.

References

URLs correct as at October 2022

Açar KV 2017. Webcam child prostitution: An exploration of current and futuristic methods of detection. *International Journal of Cyber Criminology* 11(1): 98–109. https://doi.org/10.5281/zenodo.495775

Aebi M, Plattner B, Ernest M, Kaszynski K & Bessler C 2014. Criminal history and future offending of juveniles convicted of the possession of child pornography. *Sexual Abuse: A Journal of Research and Treatment* 26(4): 375–390. https://doi.org/10.1177/1079063213492344

Allen E 2021. Defending the privacy of child sexual abuse victims online, in the EU and worldwide. https://www.weprotect.org/blog/defending-the-privacy-of-child-sexual-abuse-victims-online-in-the-eu-andworldwide/

Amnesty International 2016. Easy guide to encryption and why it matters. London: Amnesty International. https://www.amnesty.org/en/latest/campaigns/2016/10/easy-guide-to-encryption-and-why-it-matters/

Australian Bureau of Statistics 2020. *Crime victimisation, Australia, 2018–2019*. ABS cat. no. 4530.0. Canberra: ABS. https://www.abs.gov.au/ausstats/abs@.nsf/mf/4530.0

Babchishin KM, Hanson RK & VanZuylen H 2015. Online child pornography offenders are different: A meta-analysis of the characteristics of online and offline sex offenders against children. *Archives of Sexual Behavior* 44(1): 45–66. https://doi.org/10.1007/s10508-014-0270-x

Balfe M et al. 2015. Internet child sex offenders' concerns about online security and their use of identity protection technologies: A review. *Child Abuse Review* 24: 427–439. https://doi.org/10.1002/car.2308

Bourke ML, Frogmeli L, Detar PJ, Sullivan MA, Meyle E & O'Riordan M 2015. The use of tactical polygraph with sex offenders. *Journal of Sexual Aggression* 21(3): 354–367. https://doi.org/10.1080/13552600.2014.886729

Brown R & Bricknell S 2018. What is the profile of child exploitation material offenders? *Trends & issues in crime and criminal justice* no. 564. Canberra: Australian Institute of Criminology. https://www.aic.gov.au/publications/tandi/tandi564

Brown R, Napier S & Smith RG 2020. Australians who view live streaming of child sexual abuse: An analysis of financial transactions. *Trends & issues in crime and criminal justice* no. 589. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti04336

Bursztein E, Clarke E, DeLaune M, Elifff DM, Hsu N, Olson L, Shehan J, Thakur M, Thomas K & Bright T 2019. Rethinking the detection of child sexual abuse imagery on the internet. International World Wide Web Conference, San Francisco, 13–17 May: 2601–2607. https://doi.org/10.1145/3308558.3313482

Cashmore J & Shackel R 2013. *The long-term effects of child sexual abuse*. Child Family Community Australia paper no. 11. Melbourne: Australian Institute of Family Studies. https://aifs.gov.au/cfca/publications/long-term-effects-child-sexual-abuse

Dowling C, Boxall H, Pooley K, Long C & Franks C 2021. Patterns and predictors of reoffending among child sexual offenders: A rapid evidence assessment. *Trends & issues in crime and criminal justice* no. 632. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti78306

ECPAT International 2017. *Online child sexual exploitation: An analysis of emerging and selected issues.* ECPAT International Journal 12: 1–63. https://humantraffickingsearch.org/resource/online-child-sexual-exploitation-analysis-emerging-selected-issues/

Eke A, Helmus L & Seto M 2019. A validation study of the Child Pornography Offender Risk Tool (CPORT). *Sexual Abuse* 31(4): 456–476. https://doi.org/10.1177/1079063218762434

Elliott IA, Mandeville-Norden R, Rakestrow-Dickens J & Beech AR 2019. Reoffending rates in a UK community sample of individuals with convictions for indecent images of children. *Law and Human Behavior* 43(4): 369. https://doi.org/10.1037/lhb0000328

eSafety Commission 2020. End-to-end encryption trends and challenges: Position statement. Sydney: eSafety Commissioner. https://www.esafety.gov.au/about-us/tech-trends-and-challenges/end-end-encryption

Europol 2020. *Exploiting isolation: Offenders and victims of online child sexual abuse during the COVID-19 pandemic*. The Hague: Europol. https://www.europol.europa.eu/publications-documents/exploiting-isolation-offenders-and-victims-of-online-child-sexual-abuse-during-covid-19-pandemic

Europol 2019. *Internet organised crime threat assessment 2019*. The Hague: Europol. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019

Europol 2017. *Online sexual coercion and extortion as a form of crime affecting children: Law enforcement perspective*. The Hague: Europol. https://www.europol.europa.eu/publications-events/publications/online-sexual-coercion-and-extortion-form-of-crime-affecting-children-law-enforcement-perspective

Facebook nd. Community standards enforcement report: Child endangerment: Nudity and physical abuse and sexual exploitation. https://transparency.fb.com/data/community-standards-enforcement/child-nudity-and-sexual-exploitation/facebook/

Farid H 2019. *Testimony: House Committee on Energy and Commerce: Fostering a healthier internet to protect consumers*. Washington DC: House Committee on Energy and Commerce. https://energycommerce.house.gov/committee-activity/hearings/hearing-on-fostering-a-healthier-internet-to-protect-consumers

Gewirtz-Meydan A, Walsh W, Wolak J & Finkelhor D 2018. The complex experience of child pornography survivors. *Child Abuse & Neglect* 80: 238–248. https://doi.org/10.1016/j.chiabu.2018.03.031

Grant B, Shields B, Tabachnick J & Coleman J 2019. “I didn’t know where to go”: An examination of Stop It Now!’s sexual abuse prevention helpline. *Journal of Interpersonal Violence* 34(20): 4225–4253. https://doi.org/10.1177/0886260519869237

Goller A, Jones R, Dittman V, Taylor P & Graf M 2016. Criminal recidivism of illegal pornography offenders in the overall population: A national cohort study of 4612 offenders in Switzerland. *Advances in Applied Sociology* 6(2): 48–56. https://doi.org/10.4236/aasoci.2016.62005

Hailes H, Yu R, Danese A & Fazel S 2019. Long-term outcomes of childhood sexual abuse: An umbrella review. *The Lancet: Psychiatry* 6(10): 830–839. https://doi.org/10.1016/S2215-0366(19)30286-X

Henshaw M, Ogloff JRP & Clough JA 2018. Demographic, mental health, and offending characteristics of online child exploitation material offenders: A comparison with contact-only and dual sexual offenders. *Behavioral Sciences & the Law* 36(2): 198–215. https://doi.org/10.1002/bsl.2337

Hirschtritt ME, Tucker D & Binder RL 2019. Risk Assessment of Online Child Sexual Exploitation Offenders. *Journal of the American Academy of Psychiatry and the Law* 47(2): 155–164. https://pubmed.ncbi.nlm.nih.gov/30988020/

Insoll T, Ovaska AK, Nurmi J, Aaltonen M & Vaaranen-Valkonen N 2022. Risk factors for child sexual abuse material users contacting children online: Results of an anonymous multilingual survey on the dark web. *Journal of Online Trust & Safety* 1(2). https://doi.org/10.54501/jots.v1i2.29

International Justice Mission (IJM) 2020. *Online sexual exploitation of children in the Philippines: Analysis and recommendations for governments, industry and civil society: Summary report*. IJM. https://www.ijm.org/vawc/blog/osec-study

Internet Watch Foundation (IWF) 2018. *Trends in child sexual exploitation: Examining the distribution of captures of live-streamed child sexual abuse.* Cambridge, UK: Internet Watch Foundation. https://www.iwf.org.uk/about-us/why-we-exist/our-research/

Interpol 2020. *Threats and trends: Child sexual exploitation and abuse: COVID-19 impact.* Lyon: Interpol. https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-highlights-impact-of-COVID-19-onchild-sexual-abuse

Jung S, Ennis L, Stein S, Choy AL & Hook T 2013. Child pornography possessors: Comparisons and contrasts with contact- and non-contact sex offenders. *Journal of Sexual Aggression* 19(3): 295–310. https://doi.org/10.1080/13552600.2012.741267

Kent G 2021. Messenger policy workshop: Future of private messaging. https://about.fb.com/news/2021/04/messenger-policy-workshop-future-of-private-messaging/

Krone T, Smith RG, Cartwright J, Hutchings A, Tomison A & Napier S 2017. *Online child sexual exploitation offenders: A study of Australian law enforcement data.* Report to the Criminology Research Advisory Council. CRG 58/12–13. Canberra: Australian Institute of Criminology. https://www.aic.gov.au/crg/reports/crg-5812-13

Krone T & Smith RG 2017. Trajectories in online child sexual exploitation offending in Australia. *Trends and issues in crime and criminal justice* no. 524. Canberra: Australian Institute of Criminology. https://www.aic.gov.au/publications/tandi/tandi524

Laajasalo T, Ellonen N, Korkman J, Pakkanen T & Aaltonen O-P 2020. Low recidivism rates of child sex offenders in a Finnish 7-year follow-up. *Nordic Journal of Criminology* 21(1): 103–111. https://doi.org/10.1080/2578983X.2020.1730069

Lussier P, Deslauriers-Varin N & Râtel T 2010. A descriptive profile of high-risk sex offenders under intensive supervision in the province of British Columbia, Canada. *International Journal of Offender Therapy and Comparative Criminology* 54(1): 71–91. https://doi.org/10.1177/0306624x08323236

Morgan A 2022. *Exploring the role of opportunity in recidivist child sexual offending.* Research Report no. 24. Canberra: Australia Institute of Criminology. https://doi.org/10.52922/rr78719

Murdoch L 2016. Australian accused of child sex tourism arrested in the Philippines. *Sydney Morning Herald*, 1 September. https://www.smh.com.au/world/australian-accused-of-child-sex-tourism-arrested-in-thephilippines-20160901-gr6x8x.html

Napier S, Teunissen C & Boxall H 2021. Live streaming of child sexual abuse: An analysis of offender chat logs. *Trends & issues in crime and criminal justice* no. 639. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti78375

National Centre for Missing and Exploited Children (NCMEC) 2022a. CyberTipline 2021 report. https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata

National Center for Missing and Exploited Children 2022b. Sextortion. National Center for Missing and Exploited Children. https://www.missingkids.org/theissues/sextortion

National Center for Missing and Exploited Children (NCMEC) 2021. 2020 CyberTipline reports by electronic service providers (ESP). https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata#reports

National Center for Missing and Exploited Children (NCMEC) 2019. NCMEC's statement regarding end-to-end encryption. https://www.missingkids.org/blog/2019/post-update/end-to-end-encryption

Netclean 2020. *Netclean report: COVID-19 impact 2020: A report about child sexual abuse crime.* https://www.netclean.com/knowledge

Netclean 2019. *Netclean report 2019: A report about child sexual abuse crime.* https://www.netclean.com/knowledge

Ogloff J, Cutajar M, Mann E & Mullen P 2012. Child sexual abuse and subsequent offending and victimisation: A 45 year follow-up study. *Trends & issues in crime and criminal justice* no. 440. Canberra: Australian Institute of Criminology. https://www.aic.gov.au/publications/tandi/tandi440

Patchin J & Hinduja 2020. Sextortion among adolescents: Results from a national survey of U.S. youth. *Sexual Abuse* 32(1): 30–54. https://doi.org/10.1177/1079063218800469

Prichard J & Spiranovic C 2014. *Child exploitation material in the context of institutional child sexual abuse*. Report for the Royal Commission into Institutional Responses to Child Sexual Abuse. https://www.childabuseroyalcommission.gov.au/research

Prichard J, Wortley R, Watters P, Spiranovic C, Hunn C & Krone T 2022. Effects of automated messages on internet users attempting to access "barely legal" pornography. *Sexual Abuse* 34(1): 106–124. https://doi.org/10.1177/10790632211013809

Salter M & Hanson E 2021. "I need you all to understand how pervasive this issue is": User efforts to regulate child sexual offending on social media. In J Baily, A Flynn & N Henry (eds), *The Emerald international handbook of technology facilitated violence and abuse*. Emerald Publishing: 729–748. https://doi.org/10.1108/978-1-83982-848-520211053

Schiemer J 2018. Strong and responsible: Can encryption be both? *FlagPost*, 3 October. https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/FlagPost/2018/October/Encryption

Seto M & Eke A 2015. Predicting recidivism among adult male child pornography offenders: Development of the Child Pornography Offender Risk Tool (CPORT). *Law and Human Behaviour* 39(4): 416–429. https://doi.org/10.1037/lhb0000128

Seto MC, Hanson RK, & Babchishin KM 2011. Contact sexual offending by men arrested for child pornography offenses. *Sexual Abuse: A Journal of Research and Treatment* (23): 124–145. https://doi.org/10.1177%2F1079063210369013

Soldino V, Carbonell-Vayá E & Seigfried-Spellar K 2019. Criminological differences between child pornography offenders arrested in Spain. *Child Abuse & Neglect* 98: 104–178. https://doi.org/10.1016/j.chiabu.2019.104178

Statista 2022a. Most popular global mobile messenger apps as of January 2022, based on number of monthly active users (in millions). https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/

Statista 2022b. Number of Instagram users worldwide from 2020 to 2025 (in millions). https://www.statista.com/statistics/183585/instagram-number-of-global-users/

Stevens D 2020. Consumers seek out apps with enhanced privacy features to keep in touch in our new normal. https://www.data.ai/en/insights/market-data/consumers-seek-enhanced-privacy-app-features/

Terre des Hommes 2014. *Webcam child sex tourism: Becoming Sweetie: A novel approach to stopping the global rise of webcam child sex tourism.* The Hague: Terre des Hommes. https://www.terredeshommes.org/wp-content/uploads/2013/11/Webcam-child-sex-tourism-terre-des-hommes-NL-nov-2013.pdf

Teunissen C, Boxall H, Napier S & Brown R 2022. The sexual exploitation of Australian children on dating apps and websites. *Trends & issues in crime and criminal justice* no. 658. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti78757

Teunissen C & Napier S 2022. Child sexual abuse material and end-to-end encryption on social media platforms: An overview. *Trends & issues in crime and criminal justice* no. 653*.* Canberra: Australian Institute of Criminology. http://doi.org/10.52922/ti78634

Teunissen C & Napier S forthcoming. The co-occurrence of child sexual abuse live streaming and other forms of child exploitation. *Trends & issues in crime and criminal justice*. Canberra: Australian Institute of Criminology

Tidy J 2021. Omegle: Children expose themselves on video chat site*. BBC News*, 18 February. https://www.bbc.com/news/technology-56085499

Torres-Cortez R 2022. 'Sextortion' crimes against children increasing, FBI says. *Las Vegas Review-Journal*, 5 May. https://www.reviewjournal.com/crime/sex-crimes/sextortion-crimes-against-children-increasing-fbi-says-2572147/

Voreacos D 2019. U.S., South Korea bust giant child porn site by following a Bitcoin trail. *Bloomberg*, 17 October. https://www.bloomberg.com/news/articles/2019-10-16/giant-child-porn-site-is-busted-as-u-s-follows-bitcoin-trail

Wakefield J 2021. Apple delays plan to scan iPhones for child abuse. *BBC News*, 3 September. https://www.bbc.com/news/technology-58433647

WhatsApp 2020. Two billion users – Connecting the world privately. https://blog.whatsapp.com/two-billion-users-connecting-the-world-privately

Wolak JD, Finkelhor D, Walsh W & Treitman L 2018. Sextortion of minors: Characteristics and dynamics. *Journal of Adolescent Health* 62(1): 72–79. https://doi.org/10.1016/j.jadohealth.2017.08.014

Woodhams J, Kloess JA, Jose B & Hamilton-Giachritsis CE 2021. Characteristics and behaviors of anonymous users of dark web platforms suspected of child sexual offenses. *Frontiers in Psychology* 12: 623–668. https://doi.org/10.3389/fpsyg.2021.623668

Appendix: Recent and forthcoming AIC research on child sexual exploitation

Brown R & Bricknell S 2018. What is the profile of child exploitation material offenders? *Trends & issues in crime and criminal justice* no. 564. Canberra: Australian Institute of Criminology. https://www.aic.gov.au/publications/tandi/tandi564

Brown R, Napier S & Smith RG 2020. Australians who view live streaming of child sexual abuse: An analysis of financial transactions. *Trends & issues in crime and criminal justice* no. 589. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti04336

Brown R & Shelling J 2019. Exploring the implications of child sex dolls. *Trends & issues in crime and criminal justice* no. 570. Canberra: Australian Institute of Criminology. https://www.aic.gov.au/publications/tandi/tandi570

Cale J Holt T, Leclerc B, Singh S & Drew J 2021. Crime commission processes in child sexual abuse material production and distribution: A systematic review. *Trends & issues in crime and criminal justice* no. 617. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti04893

Cubitt T, Napier S & Brown R 2021. Predicting prolific live streaming of child sexual abuse. *Trends & issues in crime and criminal justice* no. 634. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti78320

Dowling C, Boxall H, Pooley K, Long C & Franks C 2021. Patterns and predictors of reoffending among child sexual offenders: A rapid evidence assessment. *Trends & issues in crime and criminal justice* no. 632. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti78306

Dowling C, Morgan A & Pooley K 2021. Reoffending among child sexual offenders. *Trends & issues in crime and criminal justice* no. 628. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti78085

Eggins E et al. 2021. Criminal justice responses to child sexual abuse material offending: A systematic review and evidence and gap map. *Trends & issues in crime and criminal justice* no. 623. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti78023

Henshaw M, Arnold C, Darjee R, Ogloff J & Clough J 2020. Enhancing evidence-based treatment of child sexual abuse material offenders: The development of the CEM-COPE Program. *Trends & issues in crime and criminal justice* no. 607. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti04787

Leclerc B, Drew J, Holt T, Cale J & Singh S 2021. Child sexual abuse material on the darknet: A script analysis of how offenders operate. *Trends & issues in crime and criminal justice* no. 627. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti78160

Lyneham S & Facchini L 2019. Benevolent harm: Orphanages, voluntourism and child sexual exploitation in South-East Asia. *Trends & issues in crime and criminal justice* no. 574. Canberra: Australian Institute of Criminology. https://www.aic.gov.au/publications/tandi/tandi574

McKillop N, Rayment-McHugh S, Smallbone S & Bromham Z 2018. Understanding and preventing the onset of child sexual abuse in adolescence and adulthood. *Trends & issues in crime and criminal justice* no. 554. Canberra: Australian Institute of Criminology. https://www.aic.gov.au/publications/tandi/tandi554

Morgan A 2022. *Exploring the role of opportunity in recidivist child sexual offending.* Research Report no. 24. Canberra: Australia Institute of Criminology. https://doi.org/10.52922/rr78719

Napier S, Teunissen C & Boxall H 2021. Live streaming of child sexual abuse: An analysis of offender chat logs. *Trends & issues in crime and criminal justice* no. 639. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti78375

Napier S, Teunissen C & Boxall H 2021. How do child sexual abuse live streaming offenders access victims? *Trends & issues in crime and criminal justice* no. 642. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti78474

Prichard J et al. 2022. Warning messages to prevent illegal sharing of sexual images: Results of a randomised controlled experiment. *Trends & issues in crime and criminal justice* no. 647. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti78559

Salter M, Wong WKT, Breckenridge J, Scott Sue, Cooper S & Peleg N 2021. Production and distribution of child sexual abuse material by parental figures. *Trends & issues in crime and criminal justice* no. 616. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti04916

Salter M & Woodlock D forthcoming. Secrecy, control and violence in women's intimate relationships with child sexual abuse material offenders. *Trends & issues in crime and criminal justice*. Canberra: Australian Institute of Criminology

Teunissen C, Boxall H, Napier S & Brown R 2022. The sexual exploitation of Australian children on dating apps and websites. *Trends & issues in crime and criminal justice* no. 658. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti78757

Teunissen C & Napier S 2022. Child sexual abuse material and end-to-end encryption on social media platforms: An overview. *Trends & issues in crime and criminal justice* no. 653. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti78634

Teunissen C & Napier S forthcoming. How is live streaming of child sexual abuse linked with other forms of child sexual offending? An analysis of offender chat logs. *Trends & issues in crime and criminal justice*. Canberra: Australian Institute of Criminology

Westlake B et al. 2022. Developing automated methods to detect and match face and voice biometrics in child sexual abuse videos. *Trends & issues in crime and criminal justice* no. 648. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti78566

Sarah Napier is the Manager of the Online Sexual Exploitation of Children Research Program at the Australian Institute of Criminology.

Dr Rick Brown is the Deputy Director of the Australian Institute of Criminology.