Submission to Australian Joint Standing Committee on Law Enforcement

Inquiry into law enforcement capabilities in relation to child exploitation

AUGUST 2021

FACEBOOK

Executive summary

Facebook welcomes the opportunity to provide a submission to the Joint Standing Committee on Law Enforcement's inquiry into *Law enforcement capabilities in relation to child exploitation*. The terms of reference for the inquiry refer to child sexual abuse material (CSAM) available on digital services and, given Facebook's significant efforts in combatting CSAM on our services, our submission is intended to assist the Joint Standing Committee by providing information about proactive steps being taken by industry.

Using the internet to harm children is abhorrent and unacceptable, and there is a continuous responsibility for all stakeholders - government, industry, and the broader community - to work together to protect children. Facebook has been an industry leader in initiatives to combat child exploitation, focussed especially on detecting, removing and reporting online CSAM on our services. Offenders can quickly change tactics to avoid detection, and we take responsibility for detecting and removing them from Facebook's services.

In this submission, we outline the approach that Facebook takes to protecting children on our services. We have significantly increased our commitments and investments in this area in recent years, and we now have 35,000 people working on safety and security within Facebook.

Our strategy is based on four elements: developing **policies**, developing technology to **enforce** our policies by detecting and removing violating content, providing **tools** to support Australians to have a safe and positive experience on our services, and establishing **partnerships** with NGOs, other digital platforms and governments to encourage collaboration in protecting children online.

The impact of our efforts is clear: in the last quarter alone, we removed 25.7 million pieces of content for child sexual exploitation, and 99.5% of this content was detected and removed by us proactively before a user needed to see it and report it to us.[1] When we detect CSAM, we report it to the non-government organisation (NGO) the National Center for Missing and Exploited Children (NCMEC), a nonprofit that refers cases to law enforcement in Australia and around the world, in compliance with US law.

The technology we have invested in to detect and remove CSAM is cutting edge. For example, we have developed two technologies (called PDQ and TMK+PDQF) to detect identical and near-identical photos and videos -- and we have made these technologies available open source for free to allow industry partners, small developers and NGOs to benefit from this technology too. The President and CEO of NCMEC John Clarke said, "We're confident that Facebook's generous contribution of this open-source technology will ultimately lead to the identification and rescue of

[1] Facebook, *Community Standards Enforcement Report Q2 2021 - Child nudity and sexual exploitation*, https://transparency.fb.com/data/community-standards-enforcement/child-nudity-and-sexual-exploitation/facebook/.

more child sexual abuse victims."[2] The Australian Federal Police have reviewed these algorithms and are now using them as part of their work to protect children within Australia.[3]

We're going even further to develop tools to prevent inappropriate interactions between adults and minors on our services. We recently announced that we are identifying those accounts that exhibit potentially suspicious behaviour and stopping those people from interacting with young people.[4] Australia is one of the first countries in the world where we are rolling out this capability.

We are continuing to apply this type of innovative thinking as technology evolves. For example, we know that end-to-end encryption provides the strongest possible protection from cybersecurity threats and has become the industry standard for many applications, including private messaging. However, encryption poses legitimate policy questions about how to protect the safety of users if only the recipient sees the content of private messages. The type of technology that we have developed around inappropriate interactions with young people works without needing to see the content of private messages, demonstrating that there continues to be significant innovation in how to combat CSAM online.

The relationship between technology companies and law enforcement continues to be essential to stopping offenders from abusing our services, and we look forward to opportunities to deepen that engagement further.

[2] A Davis and G Rosen, 'Open-Sourcing Photo- and Video-Matching Technology to Make the Internet Safer', *Facebook Newsroom*, 1 August 2019, https://about.fb.com/news/2019/08/open-source-photo-video-matching/.
[3] J Dalins, C Wilson and D Boudry, 'PDQ & TMK+PDQF - A test drive of Facebook's perceptual hashing algorithms', *Journal of Digital Investigations*, pre-print, submitted December 2019.
[4] Facebook, 'Giving young people a safer, more private experience on Instagram', *Facebook Newsroom*, 27 July 2021, https://about.fb.com/news/2021/07/instagram-safe-and-private-for-young-people/.

Table of contents

Introduction

Using our apps to harm children is abhorrent and unacceptable. Facebook thinks about our efforts to combat online CSAM as falling in three areas:

- We want to **prevent** abuse of our services in this way in the first place.
- If an offender circumvents our prevention efforts, we want to **detect** that content or behaviour.
- Once abuse is detected, we **respond** by reporting that material to NCMEC, which provides it onto law enforcement.

We've also undertaken in-depth analysis to understand how and why people share child exploitative content on Facebook's services. As part of this, we analysed a sample of our reports to NCMEC and found that most of the CSAM on our services were copies of known material:

- More than 90% of our NCMEC reports were the same or visually similar to material that had been previously reported to NCMEC.
- More than half of the child exploitative content we reported were copies of just **six** videos.[5]

From this, we can understand that the number of pieces of CSAM content does not equal the number of victims. Instead, this suggests the behaviour that occurs on our services is largely revictimisation of the same victim by repeatedly sharing the same content.

Whilst every sharing of child exploitative content is inexcusable and harmful, analysing the nature of our reports assists us to identify that, to effectively stop this sharing of CSAM, we need to understand the intent behind the sharers. We worked with global child safety experts - including NCMEC - to develop a taxonomy of people's intent in sharing this material, based on existing research.[6] People who share these images are not a homogenous group; there are a variety of intentions. As well as those who have malicious intent towards children, people may share CSAM with nonmalicious intent (for example, out of shock or outrage, out of ignorance, in poor humour [eg. someone sharing an image of a child's genitals being bitten by an animal], or children sending sexual imagery of themselves to another child). While our work to understand intent is still ongoing, our initial estimates suggest that 75 per cent of CSAM sharing on our services is due to people sharing it with non-malicious intent.

It is analysis and understanding like this that has informed the comprehensive approach we've taken to combatting child exploitation and sharing of CSAM on our services.

[5] A Davis, 'Preventing child exploitation on our apps', *Facebook Newsroom*, 23 February 2021, https://about.fb.com/news/2021/02/preventing-child-exploitation-on-our-apps/ .

[6] J Buckley, M Andrus and C Williams, 'Understanding the intentions of Child Sexual Abuse Material (CSAM) sharers;, *Facebook Research Blog*, 23 February 2021, https://research.fb.com/blog/2021/02/understanding-the-intentions-of-child-sexual-abuse-material-csam-sharers/.

Facebook's work in combatting child exploitation

Our work to combat child exploitation falls in four broad categories:

1. **Policies** to set out what material is and is not allowed on our services
2. **Enforcement** of those policies via advanced technology
3. **Tools** to support Australians to have a safe and positive experience on our services
4. **Partnerships** with NGOs, other digital platforms, and governments to encourage collaboration in protecting children online.

Each of these is outlined in more detail below.

Policies

The policies about what material is and is not allowed on Facebook is contained in our Community Standards.[7] We have long had a very clear policy that CSAM is not permitted on our services. This policy is broader than just material that depicts sexual intercourse; we also do not allow:

- Child nudity
- Content that involves a child and includes sexual elements (for example, restraints, a focus on genitals, presence of an aroused adult, presence of sex toys, sexualised costumes, stripping, a staged environment or professionally shot, or open-mouth kissing)
- Content of children in a sexual fetish context
- Content that supports, promotes, advocates or encourages participation in paedophilia
- Content that identifies or mocks alleged victims of child sexual exploitation by name or image
- Solicitation content (for example, soliciting imagery of child sexual exploitation or real-world sexual encounters with children)
- Content that constitutes or facilitates inappropriate interactions with children (for example, engaging in implicitly sexual conversation with children or obtaining or requesting sexual material from children).

There are adjacent types of content that we also do not allow on our services. For example, in 2020, we expanded our policies to prohibit the implicit sexualisation of minors (in addition to our pre-existing policies against the explicit sexualisation of children). This can be a challenging category of material to detect that requires fine judgements to be made: for example, a user who comments on a benign photo of a child by saying it is "beautiful" could be, depending on the context, either providing an innocent compliment or inappropriately sexualising a child.

We also restrict the display of nudity or sexual activity of adults more generally, and content that involves the non-sexual abuse of children.

[7] Facebook, *Community Standards*, https://www.facebook.com/communitystandards/.

These policies are developed in close consultation with global experts, including in Australia. We convene a global Safety Advisory Board (which contains Australian experts, like PROJECT ROCKIT), quarterly virtual roundtables with Australian stakeholders, and specific consultation with subject matter experts when we're considering potential policy changes.

Enforcement

In order to enforce our policies, we investigate very significantly in both technology and people to help detect violating content, or suspicious behaviour.

Firstly, we build up teams of experts who work in this space. The number of people working on safety and security has increased to more than 35,000 in recent years.

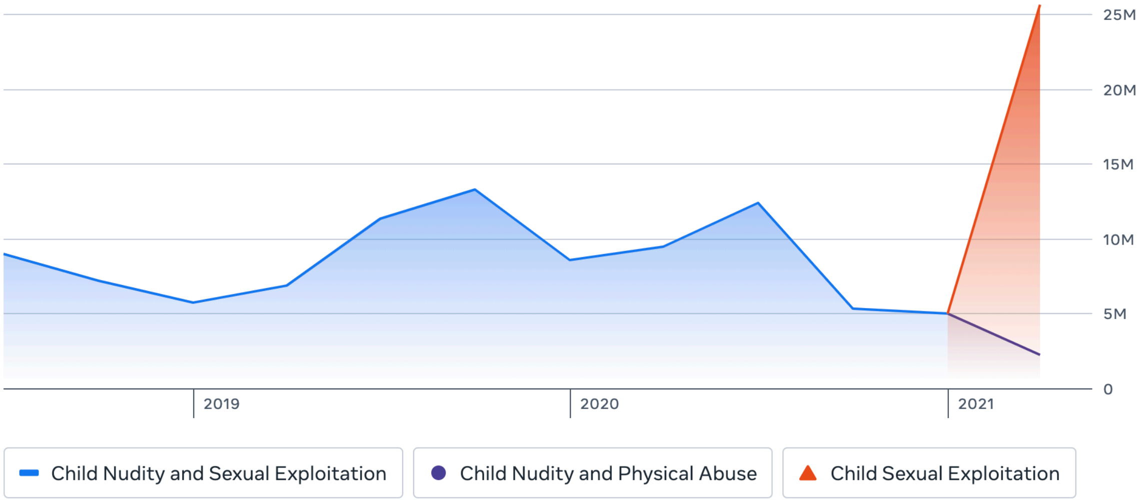
Secondly, the technology we have invested in to detect and remove CSAM is cutting edge. For example, we have developed two technologies (called PDQ and TMK+PDQF) to detect identical and near-identical photos and videos -- and we have made these technologies available open source for free to allow industry partners, small developers and NGOs to benefit from this technology too. The President and CEO of NCMEC John Clarke said, "We're confident that Facebook's generous contribution of this open-source technology will ultimately lead to the identification and rescue of more child sexual abuse victims."[8] The Australian Federal Police have reviewed these algorithms and are now using them as part of their work to protect children within Australia. We use these technologies along with many other examples of artificial intelligence.

Our work has a significant impact. In the last quarter alone, we removed 25.7 million pieces of content for child sexual exploitation, and 99.5% of this content was detected and removed by us proactively before a user needed to see it and report it to us.[9] For many years, we have detected millions of pieces of CSAM, consistently more than 99% detected proactively by us before users report it to us, which requires them to have seen it first.

[8] A Davis and G Rosen, 'Open-Sourcing Photo- and Video-Matching Technology to Make the Internet Safer', *Facebook Newsroom*, 1 August 2019, https://about.fb.com/news/2019/08/open-source-photo-video-matching/.

[9] Facebook, *Community Standards Enforcement Report Q2 2021*, https://transparency.fb.com/data/community-standards-enforcement/child-nudity-and-sexual-exploitation/facebook/.

Graph 1: Volume of child endangerment content detected and removed from Facebook 2018-2021



Note: From Q2 2021, we have broken out and reported separately on child sexual exploitation versus child nudity. Prior to this time, both categories of content were reported together.

When we become aware of CSAM, we report it to the NGO the National Center for Missing and Exploited Children (NCMEC), a nonprofit that refers cases to law enforcement in Australia and around the world, in compliance with US law. Facebook works closely with NCMEC to improve the ecosystem to fight this abuse, for example, by recently rebuilding their case management tool pro-bono in order to provide greater context around a particular report when it is provided to law enforcement around the world.

Tools

We offer a number of tools in this space, including:

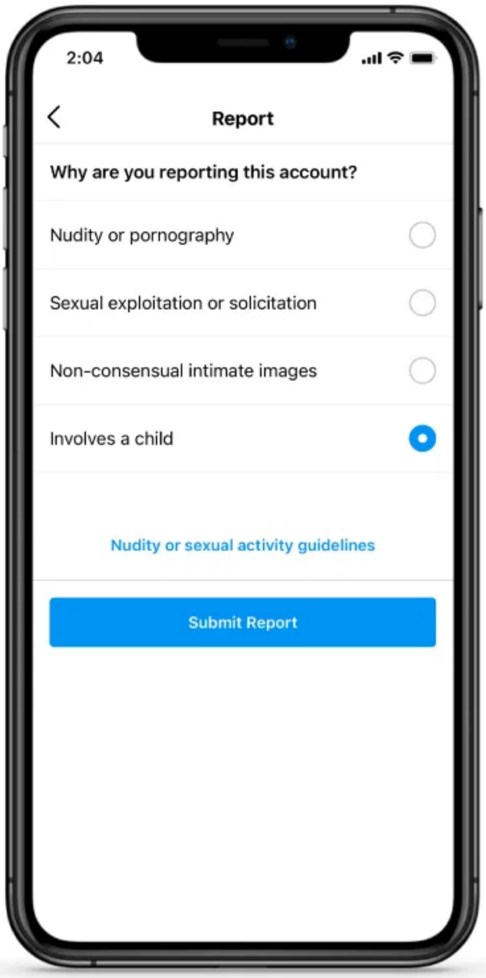
- tools for parents and young people to support them in having a safe experience on our services.
- tools to deter potential offenders.

Tools for parents and young people

We have longstanding tools that young people can take in order to protect the privacy of their own accounts, including limiting who can find them, who can send them a friend request and what information is publicly available. We've also provided longstanding options to Block, Report, Hide or Unfollow users.

We want to stop young people from hearing from adults they don't know or don't want to hear from, and we believe private accounts are the best way to prevent this from happening. Since July 2021, everyone who is under 16 years old in Australia is defaulted into a private account when they join Instagram. For young people who already have a public account on Instagram, we'll show them a notification highlighting the benefits of a private account and explaining how to change their privacy settings.[10] We have also been investing significantly in artificial intelligence in order to detect the age of young users, especially those who may be under 13 and too young to use our apps.[11]

After consultations with child safety experts and organisations, we've made it easier to report content for violating our child exploitation policies. To do this, we added the option to choose "involves a child" under the "Nudity & Sexual Activity" category of reporting in more places on Facebook and Instagram. These reports are prioritised for review.



Why are you reporting this account?

Nudity or pornography ○

Sexual exploitation or solicitation ○

Non-consensual intimate images ○

Involves a child ●

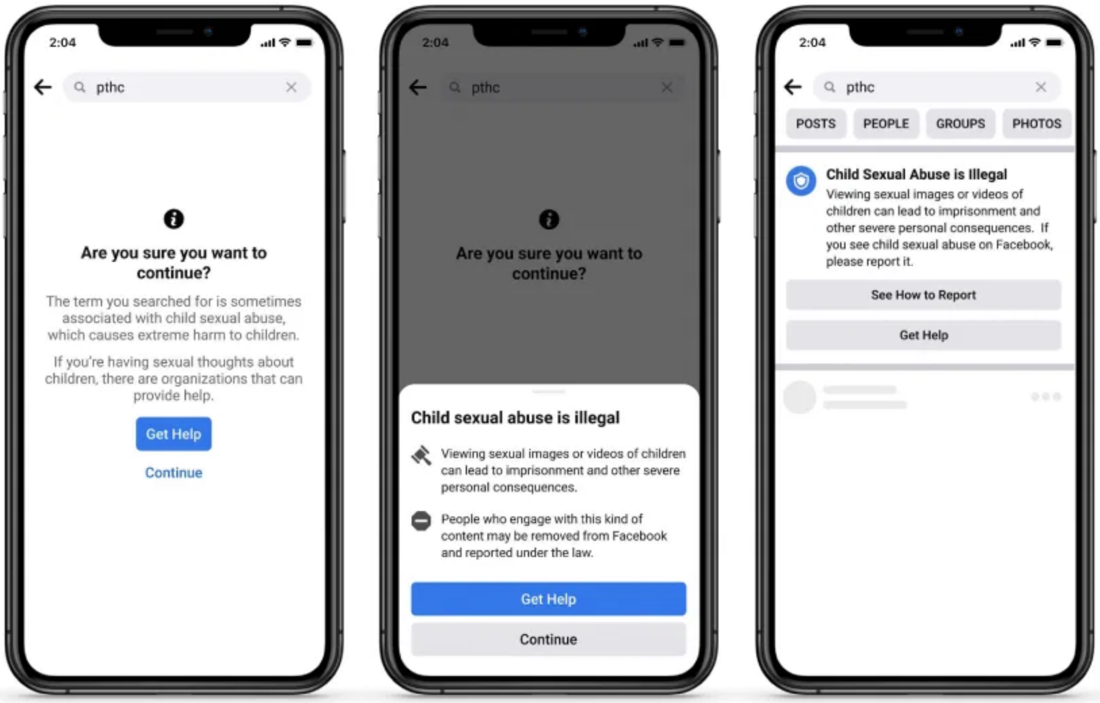
We've built a hub in our Safety Centre, dedicated to helping parents understand the various tools available to protect the safety of young people on our services. It can be accessed at www.facebook.com/safety/childsafety.

[10] Facebook, 'Giving young people a safer, more private experience on Instagram', *Facebook Newsroom*, 27 July 2021, https://about.fb.com/news/2021/07/instagram-safe-and-private-for-young-people/.
[11] P Diwanji, 'How do we know someone is old enough to use our apps?', *Facebook Newsroom*, 27 July 2021, https://about.fb.com/news/2021/07/age-verification/.

Tools to deter potential offenders

Based on our research and analysis about users with potentially malicious vs non-malicious intent, we have a range of customised interventions for users who may be looking for CSAM on our services.

We've started by testing two new tools — one aimed at the potentially malicious searching for this content and another aimed at the non-malicious sharing of this content. The first is a pop-up that is shown to people who search for terms on our apps associated with child exploitation. The pop-up offers ways to get help from offender diversion organisations and shares information about the consequences of viewing illegal content.



Are you sure you want to continue?

The term you searched for is sometimes associated with child sexual abuse, which causes extreme harm to children.

If you're having sexual thoughts about children, there are organizations that can provide help.

Are you sure you want to continue?

Child sexual abuse is illegal

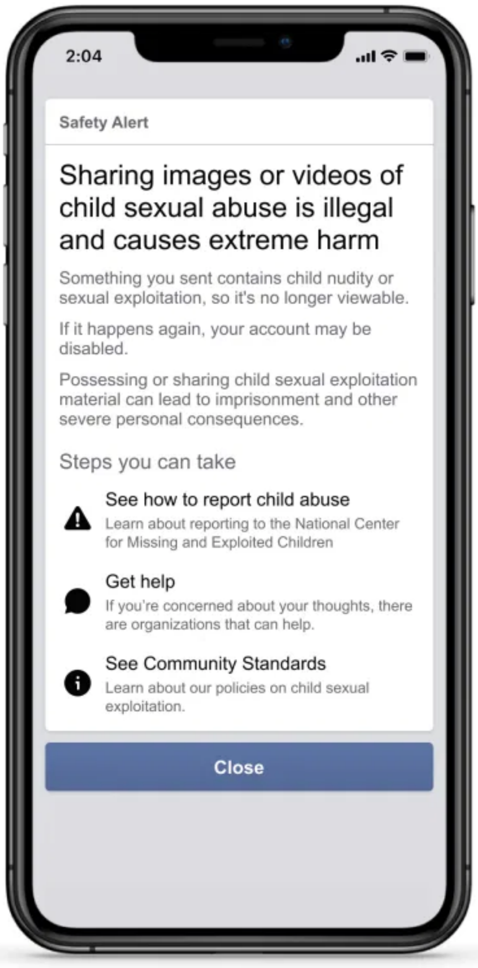
Viewing sexual images or videos of children can lead to imprisonment and other severe personal consequences.

People who engage with this kind of content may be removed from Facebook and reported under the law.

Child Sexual Abuse is Illegal

Viewing sexual images or videos of children can lead to imprisonment and other severe personal consequences. If you see child sexual abuse on Facebook, please report it.

The second is a safety alert that informs people who have shared viral, meme child exploitative content about the harm it can cause and warns that it is against our policies and there are legal consequences for sharing this material. We share this safety alert in addition to removing the content, banking it and reporting it to NCMEC. Accounts that promote this content will be removed. We are using insights from this safety alert to help us identify behavioural signals of those who might be at risk of sharing this material, so we can also educate them on why it is harmful and encourage them not to share it on any surface — public or private.



2:04

Safety Alert

Sharing images or videos of child sexual abuse is illegal and causes extreme harm

Something you sent contains child nudity or sexual exploitation, so it's no longer viewable.

If it happens again, your account may be disabled.

Possessing or sharing child sexual exploitation material can lead to imprisonment and other severe personal consequences.

Steps you can take

See how to report child abuse
Learn about reporting to the National Center for Missing and Exploited Children

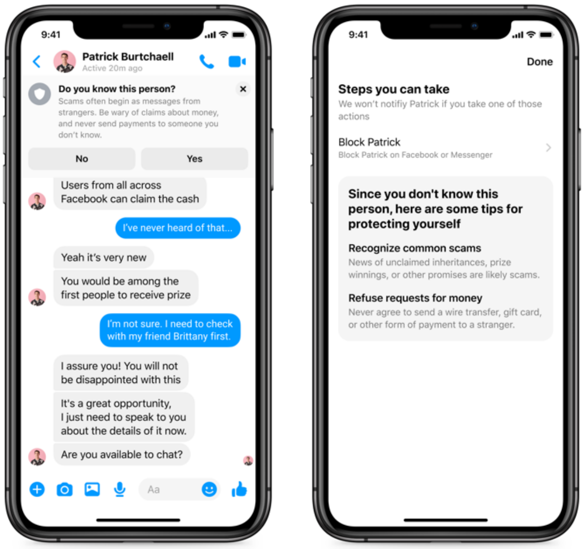
Get help
If you're concerned about your thoughts, there are organizations that can help.

See Community Standards
Learn about our policies on child sexual exploitation.

We are also taking steps to make it harder for potential suspicious accounts to contact young users. We've developed new technology that will allow us to find accounts that have shown potentially suspicious behaviour and stop those accounts from interacting with young people's accounts. By "potentially suspicious behaviour", we mean accounts belonging to adults that may have recently been blocked or reported by a young person, for example.

Using this technology, we prevent young people's accounts from appearing in recommendations to these adults. If they find young people's accounts by searching for their usernames, they aren't able to follow them. They aren't able to see comments from young people on other people's posts, nor will they be able to leave comments on young people's posts.

Since 2020, we have also sent notices to users in Messenger where we believe an adult could be pursuing a potentially inappropriate private interaction with a child. These are used in instances where someone may be grooming or scamming another user.[12]



Do you know this person?
Scams often begin as messages from strangers. Be wary of claims about money, and never send payments to someone you don't know.

Users from all across Facebook can claim the cash

I've never heard of that...

Yeah it's very new

You would be among the first people to receive prize

I'm not sure. I need to check with my friend Brittany first.

I assure you! You will not be disappointed with this

It's a great opportunity, I just need to speak to you about the details of it now.

Are you available to chat?

Steps you can take
We won't notifiy Patrick if you take one of those actions

Block Patrick
Block Patrick on Facebook or Messenger

Since you don't know this person, here are some tips for protecting yourself

Recognize common scams
News of unclaimed inheritances, prize winnings, or other promises are likely scams.

Refuse requests for money
Never agree to send a wire transfer, gift card, or other form of payment to a stranger.

Partnerships

While we undertake a lot of work to ensure our own services are safe, we know that online CSAM is an industry-wide problem and requires collaboration between digital platforms and governments, law enforcement, safety experts, NGOs and parents. It's our collective responsibility to combat abuse and protect young people online.

In 2020, we joined with Google, Microsoft and 15 other tech companies to announce the formation of "Project Protect: A plan to combat online child sexual abuse", a renewed commitment and investment from the Technology Coalition expanding its scope and impact to protect kids online and guide its work for the next 15 years.

Project Protect is focussing on five key areas:

- **Tech innovation:** Accelerating the development and usage of groundbreaking technology. All companies involved have contributed to a multi-million dollar fund to support this work
- **Collective action:** Convening tech companies, governments and civil society to create a holistic approach to tackle this issue
- **Independent research:** Funding research with the End Violence Against Children Partnership to advance our collective understanding of the

[12] J Sullivan, 'Preventing unwanted contacts and scams in Messenger', *Messenger News*, 21 May 2020, https://messengernews.fb.com/2020/05/21/preventing-unwanted-contacts-and-scams-in-messenger/.

experiences and patterns of child sexual exploitation and abuse online, and learn from effective efforts to prevent, deter and combat it

- **Information and knowledge sharing:** Enabling greater information, expertise and knowledge sharing among companies to help prevent and disrupt child sexual exploitation and abuse online
- **Transparency and accountability:** Increasing accountability and consistency across the industry through meaningful reporting of child sexual exploitation and abuse content across member platforms and services. This will be done in conjunction with WePROTECT Global Alliance.

We also work closely with a range of Australian child safety NGOs, to ensure we are able to review and consider any material they provide us.

Based on the analysis we've undertaken of the intent behind sharing of CSAM (discussed earlier), we will shortly be launching a public service announcement in a number of markets, including in Australia around National Child Protection Week. The PSA will spread the message of "report it, don't share it" in order to educate members of the community who may fall into the category of non-malicious sharers of CSAM. The PSA will direct Australians to report material they see either to Facebook or to the Office of the eSafety Commissioner.

We also work with Australian law enforcement in a variety of ways, including by helping to amplify their public service announcements. The Australian Centre for Child Exploitation has had great success using Facebook and Instagram for their recent series, which reached over 1.3 million people and increased traffic to their website 1110%. They said "Social media is having a tremendous impact in both the prevention and operational work of the ACCCE, and we thank our loyal followers and partners who are working with us to fight online child sexual exploitation and win."[13] We have also been a key sponsor for many years of Taskforce Argos' Youth Technologies and Virtual Communities Conference, a globally recognised forum that supports practitioners in the fields of law enforcement, prosecution, education, child protective services, social work, children's advocacy and therapy who work directly with child victims of crime.

We also have a range of additional partnerships to assist with education and empowerment of children and parents engaging online:

- PROJECT ROCKIT's Digital Ambassadors program, in which Facebook has invested more than $1 million. Digital Ambassadors is a youth-led, peer-based anti-bullying initiative. A Digital Ambassador aims to utilise credible strategies to safely connect and tackle online hate. We are supporting PROJECT ROCKIT to continue to reach young people through education, particularly in remote and regional areas throughout 2021. This is a nine-year partnership that has directly empowered more than 11,500 young Australians to tackle

[13] Australian Centre to Counter Child Exploitation, *Newsletter June 2021*, https://www.accce.gov.au/news-and-media/newsletter/newsletter-june-2021.

cyberbullying.[14] The most recent version of the program has been launched by the eSafety Commissioner herself.

Australian eSafety Commissioner launching the virtual version of Digital Ambassadors

JULIE-INMAN GRANT
AUSTRALIAN ESAFETY COMMISSIONER
I'm Australia's eSafety Commissioner.

- We worked with the Alannah and Madeline Foundation and the Stars Foundation on the Safe Sistas program, which supports the online safety of young Indigenous women to respond to the issue of non-consensually shared intimate images.[15]

- We supported Susan McLean and CyberSafety Solutions to deliver online education to students and parents across Australia. We supported continued education and resources for parents in a new online format, with greater capacity at the beginning of the pandemic.

- To support parents to understand the tools that are available on Instagram, we worked with ReachOut to develop an Instagram Parents Guide that contains suggested conversation starters to better understand how their teens are using Instagram and how to ensure they are using it safely and positively. We released the Guide in September 2019 and updated it in June 2021.[16]

[14] R Thomas, 'Young People at the Centre', Facebook Australia blog, 8 February 2021, https://australia.fb.com/post/young-people-at-the-centre/.
[15] Alannah & Madeline Foundation, *Helping Sistas be safer*, https://www.amf.org.au/news-events/latest-news/helping-sistas-be-safer/
[16] J Machin, 'A Parent's Guide to Instagram', *Facebook Australia blog*, 22 June 2021, https://australia.fb.com/post/a-parents-guide-to-instagram-in-partnership-with-reach-out/.

Encryption

Given the terms of reference specifically mention the impact of encryption on law enforcement, we provide some additional information about encryption and child safety here.

It is critical to acknowledge upfront that end-to-end encryption is the best security tool available to protect Australians from cybercriminals and hackers. It is an essential component of cyber security and use of end-to-end encryption is so critical that it has become the global security standard for many online services, including private messaging services. All of the top ten messaging services in Australia (such as Apple's iMessage and Signal) offer end-to-end encrypted services. Taken in aggregate, end-to-end encryption is the norm today, not the exception, and people expect their messages to be safe.

However, end-to-end encryption also poses a legitimate policy question: how to promote the safety of users if you're not able to see the content of their messages?

Some stakeholders are calling for the creation of a "backdoor" that would grant them power to read certain content. But it isn't that simple. Creating a backdoor requires building a structural weakness into a secure system used by billions of people every day. Once the weakness is there, we cannot choose who finds it. Cybercriminals are well resourced and technologically skilled: a backdoor for the good guys is just an open door for criminals. This is why Amnesty International has commented, "There is no middle ground: if law enforcement is allowed to circumvent encryption, then anybody can."[17]

UNICEF describes the debate around this issue well:

> *"End-to-end encryption is necessary to protect the privacy and security of all people using digital communication channels.* ***This includes children [emphasis added]****, minority groups, dissidents and vulnerable communities. The UN Special Rapporteur on Freedom of Expression has referred to end-to-end encryption as "the most basic building block" for security on digital messaging apps. Encryption is also important for national security.*
>
> *The debate around end-to-end encryption of digital communications has been polarized into absolutist positions. These include advocating 1) for the unlimited use of end-to-end encryption; 2) for the complete abolishment of end-to-end encryption; and 3) that law enforcement should always be able to access encrypted data and will be unable to protect the public unless it can do so. Such polarized positions ignore the complexity and nuance of the debate and act as an impediment to thoughtful policy responses. As noted by the*

[17] Amnesty International, 'Government calls for Facebook to break encryption "latest attempt to intrude on private communications"', *Amnesty International News*, 4 October 2019, https://www.amnesty.org/en/latest/news/2019/10/government-calls-for-facebook-to-break-encryption-latest-attempt-to-intrude-on-private-communications/.

> *Carnegie Endowment working group on encryption, polarized, absolutist positions in this debate should be rejected."*[18]

The solution is for law enforcement and security agencies and industry, to work towards developing even more safety mitigations and integrity tools for end-to-end encrypted services, especially when combined with the existing longstanding detection and investigation methods available to law enforcement. This Committee has an opportunity to encourage a more nuanced debate in Australia about how to ensure the safety of users in an environment where virtually all communications are end-to-end encrypted.

Facebook has been continuing our industry leadership in combatting online CSAM by innovating and testing solutions that can detect possible online CSAM and take action, even if a service is end-to-end encrypted. Some of the new innovations outlined in the earlier section, just as limiting inappropriate interactions between adults and children, are agnostic about whether the messaging service is encrypted or not.

WhatsApp has been working in this space for some time and, even though it is end-to-end encrypted, we have been disabling more than 300,000 WhatsApp accounts per month for suspected sharing of online CSAM.[19] WhatsApp has also been submitting CyberTips to NCMEC. This detection is occurring via WhatsApp using advanced technology to proactively scan unencrypted information - including user reports - and to evaluate group information and behaviour for suspected sharing of CSAM.[20]

Facebook has indicated our intention to apply end-to-end encryption to Facebook Messenger; however, we know there is more to do to work through questions about how to continue our deep commitment to child safety on end-to-end encrypted services. When we announced these changes in early 2019, we publicly committed to a multi-year process of consultation to develop the most advanced safety mitigations possible for end-to-end encryption. That consultation process has involved consultation and engagement with Australian stakeholders, and it is continuing. Continued consultation with experts will help us bring our industry-leading track record on safety to an end-to-end encrypted environment.

[18] D Kardefelt-Winther, E Day, G Berman, S Witting and A Bose on behalf of the UNICEF cross-divisional task force on child online protection, *Encryption, Privacy and Children's Right to Protection from Harm*, https://www.unicef-irc.org/publications/pdf/Encryption_privacy_and_children%E2%80%99s_right_to_protection_from_harm.pdf
[19] ASPI, *In-conversation with Will Cathcart*, https://www.youtube.com/watch?v=2KBQCsLDoBA.
[20] WhatsApp, 'How WhatsApp Helps Fight Child Exploitation', *WhatsApp Help Center*, https://faq.whatsapp.com/general/how-whatsapp-helps-fight-child-exploitation/?lang=en.

le.committee@aph.gov.au
Commonwealth Parliament of Australia
Committee Secretary
Parliamentary Joint Committee on Law Enforcement
PO Box 6100
Parliament House
Canberra ACT 2600
Phone: +61 2 6277 3419
le.committee@aph.gov.au

16th February 2023

Dear Honorable Members of the Australian Parliamentary Inquiry into Law Enforcement Capabilities in Relation to Child Exploitation,

My name is Kirra Pendergast I am the Founder of Safe on Social Media Pty Ltd.
I am writing to draw your attention to two pressing issues related to child exploitation: the prevalence of child grooming and sexual abuse on online gaming platforms, specifically Roblox, and the privacy and security risks associated with the often mandatory use of mobile applications (Apps) in childcare centres and schools in Australia.

As you are aware, the internet is constantly creating new opportunities for predators to target children and engage in grooming and sexual abuse.

The specific issue is how such behaviour happens on Roblox. Predators on Roblox use a range of tactics, including offering children money (the in-game economy is called Robux) for sexual acts, engaging in role-play games that involve sexual activity and moving conversations to other platforms such as TikTok, which may open up a video message function where children may be groomed, sextorted and threatened.

In one of many disclosures, in May 2022 I spoke at a school and an 11yr old girl presented to me after the session. She graphically described whilst she was shaking a sexual assault of her in game character on Roblox. She kept saying “it happened to me” children no longer see the world as online and off. To them it is just life. The Principal and I decided that even though it was online, it was a mandatory report. The Principal notified the parents and the authorities. I am unaware of the outcome.

To combat this problem, law enforcement must have the necessary resources and expertise to identify and apprehend these predators. This may involve working closely with companies operating online gaming platforms like Roblox to identify and report suspected abuse. It may also require investment in advanced technologies and training to track and analyse online activity, particularly on social media and messaging apps where predators often move their activities.

Additionally, we would like to raise concerns about the privacy and security risks associated with the mandatory use of Apps in childcare centres and schools. While these Apps can be convenient for parents and educators to communicate and share information, they can also pose enormous risks to children's privacy and security. We must address that childcare centres, schools, after-school care, and after-school activity providers such as dance and gym classes cannot mandate these apps to parents or guilt them into using them.

When parents or guardians sign up for the service provider's App on behalf of their child (often being told that if they don't, they will miss out), they are also aiding in the creation and building of their child's digital footprint, which the child has no control over. Sensitive information, including medical records, is also entered into the App, which third parties can access if the App's security measures are not adequate.

Moreover, many apps allow users to invite "family" to view the child's journal, which includes other children if they are featured in the child's account. More often than not, someone else is seeing the child, someone the parent or guardian has not consented to, and the child they have permission to view. This may be a significant security issue when someone who may be a predator is invited into these photographs of children going about their day at day care, primary school, after-school care, and after-school activities such as dance classes.

As we all know, predators are not looking for photos of naked children; they are just looking for children.

We all sign Permission to Publish forms for our children, and there used to be a choice. If you opted out, you would be emailed the photo or given a printed copy. But lately, Safe on Social has been contacted more and more by parents that feel discriminated against. For example, a parent got us upset that she had to pull her child from an early childhood after-school activity because she didn't agree to photos of her child being published online. She had escaped domestic violence and did not want pictures of her child online. She was told that her child could not participate if they could not be photographed and published on the business's social media pages. This must stop.

These Applications and mandating their use of them take that control away from parents who cannot make informed decisions about what or how their data and their children are being used.

Questions that need to be asked;

1. Is the App paid for by the service provider, or are they using a free version? (Remember, your data becomes the product if something is free to use. If it is paid for by the parent, the use of the data may have further protection by the Australian Information Commissioners Office.)

2. Who has access to the App and its data? Where is it stored, and can it be deleted if you or your child want it all deleted in the future?

3. How are the people accessing your and your child's data vetted?

4. Are the photos able to be saved/screenshots?

5. Is there a Social Media Policy in place that advises parents not to share photos from within the App on their personal Facebook pages if other children are in the image?

6. Does the service provider have a way to email photos to the parents if they choose not to allow their child to be published on the service provider's Facebook/Instagram, and why?

7. If an opt-out is allowed, do they take photos and blur the child's face out of things they publish online or exclude them completely? (This way, a child can still feel included, and their parents can be emailed the photo, but if blurred out, they cannot be identified online.)

8. What happens to the photos and the data when a child leaves the service provider?

9. Can a parent ask for all data to be destroyed, and if so, how does that happen and when?

10. Is the use of the App mandatory? Is there another way you and your service provider can communicate and share information without using a third-party App?

Serious questions need to be asked about the legality of the compulsory use of these Apps.

We also recommend that the government invest in ensuring that these Apps are secure and that parents and educators are adequately trained in their use.

Thank you for your attention to these matters.

Sincerely,

Kirrily (Kirra) Pendergast

Founder
Safe on Social Media Pty Ltd
The eSafety Training Company Pty Ltd

Kirra is a renowned cyber safety expert, with over 30 years of experience in the fields of cyber security, IT Business consulting, and Cyber Safety. She is also passionate about working with children and has dedicated the last 15 years of her career to educating and training people on cyber safety ranging in age from 5yrs - 75+. In 2021 she spoke to more than 106,000 young people in Schools across Australia.

As the Founder of Safe on Social, Kirra splits her time between the Asia Pacific Headquarters in Byron Bay, Australia, Safe on Social's UK, and European Headquarters in London, England, and Florence, Italy. Her experience of enduring online bullying and abuse inspired her to create Safe on Social, which has now become the largest and most trusted cyber safety education and training group of companies globally.

Kirra is a global thought leader in cyber safety, providing organisations of all sizes with cyber safety and social media risk management awareness training on an international scale. She is a dynamic and engaging public speaker and media commentator, having written for numerous media organizations and appeared on major international news channels. She is also a regular guest on podcasts across the world.

Kirra's straightforward, no-nonsense approach empowers people with knowledge, giving them the skills to consume technology positively rather than have their lives consumed by technology. Her extensive experience advising governments and organisations of all sizes for 18 years before founding Safe on Social has powered the training programs provided by the company.

In 2020, Kirra appointed a first-of-its-kind advisory committee of young people to help guide Safe on Social's work. She is known for her dedication to the cyber safety cause and expertise in every aspect of the sector, making her a highly sought-after speaker and commentator.

More information about Kirra and the Safe on Social team can be found on their website www.safeonsocial.com

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:

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

Attorney-General's Department

8 November 2022

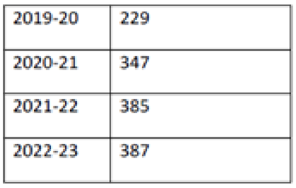
Committee Secretary
Parliamentary Joint Committee on Law Enforcement
le.committee@aph.gov.au

Dear Committee Secretary

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

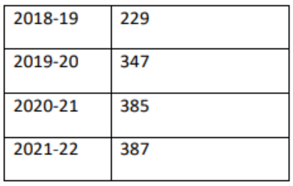
Upon additional quality assurance review of the Attorney-General's Department's submission to the Inquiry into law enforcement capabilities in relation to child exploitation, an error in the financial year timeframes table on page 4 of the submission was identified.

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

Department of Home Affairs

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

Parliamentary Joint Committee on Law Enforcement

3 September 2021

Contents

Overview

Information and communications technology have provided a vehicle for the proliferation of child sexual abuse at a global scale, and created an online market for the exchange of child abuse material, including on the darknet, where offenders can operate with anonymity. The scale of the problem continues to challenge policy and law enforcement responses. In 2020, the United States National Center for Missing and Exploited Children (NCMEC) received 21.7 million reports of child sexual abuse comprising 65.4 million images, videos and other files.

While child abuse material offenders tend to be a diverse cohort, evidence-based research is helping build a stronger picture of perpetration and trends. The scale and severity of online offending has escalated over time, with material now depicting increasingly younger children and higher degrees of violence. Concerningly, advances in technology have fuelled not only the growth of offender communities, but innovative forms of offending: for example, the use of anonymising technologies (discussed below) and a move towards new forms of financially motivated exploitation. We know that the prevalence of online child sexual abuse has increased over time, and has spiked in response to restrictions related to the COVID-19 pandemic.

Use of anonymising technologies

Organised and dangerous criminals are increasingly using anonymising technologies to conceal illicit activity and their identities. Dark Web networks have been embraced by criminals, as have capabilities such as modified mobile devices that operate on encrypted networks for criminal subscribers. These technologies can be easily combined for cumulative effect, providing multiple layers of obfuscation, making it exceedingly difficult to attribute illicit activities to specific, identifiable offenders, and impeding law enforcement capabilities to investigate serious criminality occurring online.

This situation is made worse by digital industry's adoption of encryption and anonymising technologies on their platforms. While strong encryption plays an important role in protecting user privacy and data, the use of this technology in some settings, particularly on platforms used by children, brings with it important public safety risks. The application of end-to-end encryption across social media messaging services – such as is being proposed by Facebook (including platforms such as Messenger and Instagram Direct), will provide predators with the ability to evade detection as they connect with multiple vulnerable children anywhere in the world and develop exploitative grooming relationships. The nature of end-to-end encryption means that not even Facebook, as the hosting company, would be able to retrieve or view these messages in order to detect child abuse, even with a warrant issued by a judge. The anonymity afforded by end-to-end encryption not only enables predators to groom victims on a social media platform, it also allows these criminals to safely connect and share tactics on how to perpetrate child sexual abuse, share explicit images, arrange live streaming of child sexual abuse with facilitators in vulnerable countries, and avoid law enforcement.

The anonymity offered by the dark web and other forms of anonymising technologies, combined with the rise of live-streaming and pay-per-view services, and the use of virtual currencies is making it increasingly difficult to identify and track offenders. It is often the case that IP addresses, locations and jurisdictions of users and the services used, are hidden because of this technology.

Opportunities to enhance responses

Legislative responses

Overview of existing legislation

There are three main frameworks that comprise the Australian Government's legislative toolkit for law enforcement responses to countering child sexual abuse:

- The ***Criminal Code Act 1995* (Cth)** (the Criminal Code) comprehensively criminalises conduct relating to child sexual abuse and child abuse material committed via a carriage service, such as the internet, via a postal service or by Australians overseas. The Criminal Code also makes it an offence for Australian citizens with reporting obligations recorded on a State or Territory child protection register to depart Australia without permission from authorities. These offences are contained in Divisions 271A, 272, 273, 471 (Subdivision B and C) and 474 (Subdivisions D, E and F) of the Criminal Code.
- The electronic surveillance framework, comprising the ***Telecommunications (Interception and Access) Act 1979*** and the ***Surveillance Devices Act 2004,*** creates targeted powers for law enforcement agencies to combat cyber-enabled criminality by accessing communications and gathering evidence for their investigations.
- The ***Customs Act 1901*** contains offences that prohibit the importation and exportation of child abuse material, including child-like sex dolls.

The means by which this framework enables the Commonwealth to respond to, investigate and prevent online offending are explored below. In addition to law enforcement responses, the *Online Safety Act 2021* provides the framework for regulatory responses to countering child abuse material, administered by Australia's eSafety Commissioner. The regulatory and law enforcement framework complement one another. The *Online Safety Act 2021* is outlined by the Department of Infrastructure, Transport, Regional Development and Communications in its submission to the Parliamentary Inquiry.

Criminal Code Act 1995

Child abuse material

Subdivision D of Division 474 criminalises dealings with child abuse material via a carriage service, such as the internet. Subdivision D contains offences relating to the use of a carriage service for child abuse material, including possession, production, supply and obtaining of such material. Penalties of up to 30 years' imprisonment apply to these offences. The definition of child abuse in section 473.1 is comprehensive and includes depictions, representations and descriptions of children under 18 years engaged in a sexual pose, sexual activity and subjected to torture, cruelty or physical abuse whether in animations, literature, images and videos.

In 2019 and 2020, the Australian Government strengthened child abuse material offences in the Criminal Code to address new and emerging trends. The *Combatting Child Sexual Exploitation Legislation Amendment Act 2019*, which came into force in September 2019, introduced a new offence at section 474.22A for possessing or controlling child abuse material obtained or accessed via a carriage service. This offence helped ensure that all conduct associated with the online access and possession of child abuse material is criminalised under Commonwealth law. By the end of 2020, over 70 offenders had been prosecuted under this offence.

The Act expanded the meaning of 'child abuse material' and removed references to the out-dated and inappropriate term 'child pornography'. This terminology more accurately reflects the gravity of the crimes and the harm inflicted on victims.

Why is the term 'child pornography' harmful?

Use of the phrase "child pornography" is inaccurate and benefits child sex abusers because it:

- indicates legitimacy and compliance on the part of the victim and therefore legality on the part of the abuser; and
- conjures images of children posing in 'provocative' positions, rather than suffering horrific abuse.

Every photograph or video captures an actual situation where a child has been abused.

This Act also introduced a standalone possession offence for child-like sex dolls, attracting a maximum penalty of 15 years' imprisonment. It explicitly criminalised dealings with child-like sex dolls as an emerging form of child abuse material, including importation, posting and ordering of these materials. These reforms responded to the risks identified by Brown and Shelling 2019 that child-like sex dolls could normalise abusive behaviour towards, and encourage the sexualisation of, children (Australian Institute of Criminology). They also ensure that all jurisdictions can respond to the detection of these abhorrent materials using specific criminal offences. Anecdotal reports from law enforcement indicate that child-like dolls are frequently part of a wider pattern of child sexual abuse offending, as per the case study below.

Case study: Arrest for child-like sex doll offences

Child-like sex doll offenders are a high-value target from a law enforcement and intelligence perspective. Offenders may come to the attention of law enforcement in connection with a doll-related offence, but on subsequent investigation are found to be engaging in conduct that causes direct harm to children.

An example that illustrates this is the arrest of a 60-year-old New South Wales man, who was identified when he allegedly imported a package suspected to contain a child-like sex doll. Further investigation efforts unveiled the full scope of his alleged offending, which included possession of child abuse material. Most disturbingly, however, the alleged offender was accused of having installed surveillance cameras in the bedroom of a child on a neighbouring property, and setting up a live feed to watch the footage.

In this instance, identification of the importation uncovered a broader pattern of alleged offending that may not otherwise have been revealed, allowing the Australian Border Force and police to act before a child came to harm.

The *Crimes Legislation Amendment (Sexual Crimes Against Children and Community Protection Measures) Act 2020* (Sexual Crimes Against Children Act), which came into force in June 2020, targets all parts of the criminal justice cycle for child sex offenders – from bail and sentencing through to supervision after prison time. Key child abuse material-related reforms in the Sexual Crimes Against Children Act include a new offence at section 474.23A of the Criminal Code that criminalises conduct relating to an electronic service – such as creating or moderating a website or chatroom – for the purposes of committing or facilitating the commission of child abuse material offences. Maximum penalties of 20 years imprisonment apply. This offence targets conduct whereby an individual intentionally facilitates access to child abuse.

The Act also introduced sentencing reforms to address the inadequacy of sentencing practices whereby the average length of imprisonment for a child sex offence was 18 months and nearly 40 per cent of convicted child sex offenders were spending no time in prison. Adult offenders committing the most serious Commonwealth child abuse crimes and repeat offenders will now be subject to the setting of a mandatory head sentence of 4 years, with certain exceptions. These new minimum penalties better reflect that child sexual abuse has serious and long-term impacts and online offending serves to perpetuate the market demand for child abuse material. At the time of submission, only a small number of sentences have been handed down for 'second strike' offences in relation to Commonwealth child abuse material offences.

Sexual activity (including livestreaming)

Division 474 (Subdivision F) criminalises the use of a carriage service to engage in sexual activity with a child – including 'real time' live-streamed child sexual abuse that often occurs via popular platforms such as Skype and involving children and facilitators based overseas. Penalties of up to 20 years of imprisonment apply or 30 years for aggravated offending. An offence is considered aggravated where the child has a mental impairment; is under the care or authority of the offender; is subjected to cruel, inhumane or degrading treatment in connection with the sexual activity; or dies as a result of the physical harm suffered in connection with the underlying sexual activity.

The additional aggravating factors for cruel, inhuman or degrading treatment, or where the child dies as a result of offending were added to this offence via the Sexual Crimes Against Children Act 2020 to reflect alarming trends towards offenders inflicting severe violence on children alongside sexual abuse, including in response to market demand for such depraved abuse. For example, research by the Internet Watch Foundation in 2017 based on analysis of over 2,000 images and video captures from live streamed sexual abuse of children revealed that 40 per cent were classified as containing serious sexual abuse, including the rape and torture of children.[1]

While the Commonwealth Criminal code comprehensively criminalises live-streaming of child sexual abuse, it is a challenging crime type because live-streaming leaves no visual evidence and, unless an offender records that abuse, investigators often need to rely on session logs, data usage trails and financial transactions identified as suspicious via AUSTRAC's intelligence reports (ECPAT International 2018). For more information on 'Live Online Child Sexual Abuse', see the AFP's submission to this inquiry.

Preparatory offences

Under Division 474 (Subdivision F) it is an offence, carrying a penalty of 15 years' imprisonment, to use a carriage service to:

- Procure or groom a child, or
- Groom another person to make it easier to procure a child.

Under this Subdivision, it is an offence carrying a penalty of 10 years' imprisonment to transmit an indecent communication to a child.

[1] 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

Under Division 474 (Subdivision F), it is an offence to use a carriage service to procure or groom a child under 16 years for sexual activity, groom another person to make it easier to procure a child for sexual activity, and prepare or plan to cause harm to, engage in sexual activity with, or procure for sexual activity, persons under 16 years. The offence is otherwise known as ‘Carly’s Law’.

Carly’s Law and the murder of Carly Ryan

In 2007, 15-year-old Carly Ryan was brutally murdered by Garry Francis Newman, becoming the first Australian child to be killed as a result of having been groomed online. Newman, then 50, groomed Carly over an 18-month period, posing online as an 18-year-old musician. He used this guise to lure her into meeting, leading to her tragic death.

Carly’s Law (Section 474.25C of the *Criminal Code* (Cth) was introduced via the *Criminal Code Amendment (Protecting Minors Online) Act 2017*, arming police with more power to put online predators before the courts to be held to account for their actions. Carly’s Law protects children under the age of 16 from online offenders by allowing police to focus on preparatory behaviour and act earlier in an investigation, providing avenues for disruption and prevention before an offender can cause harm to, or commits an offence against a child. The offence carries a maximum penalty of 10 years' imprisonment, and captures a broad range of conduct: for example, where an adult is communicating with a child and purporting to be younger with the intention of causing harm. The breadth of the offence enables Australian law enforcement to charge a person before they have communicated with or arranged to meet a specific child, and without having demonstrated a sexual intent.

For this reason, Carly’s Law is effective in disrupting harmful online behaviour towards children at an early stage. Because the offence covers a broad range of preparatory behaviour, offenders may first come to the attention of police for acting in suspected contravention of the offence. However, throughout the course of subsequent investigations, they frequently are found to have committed other crimes that carry more serious penalties, such as online grooming. It is an important tool that enables police to intervene early before a child comes to serious harm.

This Subdivision also criminalises the transmission of an indecent communication to a child given this is a common technique for grooming a child for sexual abuse. These offences carry a penalty of up to 10 years’ imprisonment.

Obligations for service providers

Division 474 (Subdivision E) creates obligations for providers and hosts of internet services to report child abuse material to the Australian Federal Police. It is an offence, carrying a penalty of 800 penalty units, not to comply with these obligations.

Overseas offending, and restrictions on travel by known sex offenders

Divisions 272 and 273 of the *Criminal Code* addresses offending that takes place overseas, or victimises children overseas. These offences seek to replicate domestic offences to apply to overseas contexts, by criminalising:

- The overseas sexual abuse of children by Australian citizens or residents. This includes grooming, procuring and sexual intercourse or activity with child, as well as encouraging a child sexual abuse offence. Maximum penalties of up to life imprisonment apply.
- The possession, production, distribution and procuring of child abuse material outside Australia. Maximum penalties of up to 30 years imprisonment apply.

As a means of preventing these offences, the Australian Government introduced the *Passports Legislation Amendment (Overseas Travel by Child Sex Offenders) Act* in December 2017. This placed restrictions on travel by registered child sex offenders, introducing an offence into Division 271A of the *Criminal Code Act 1995* (Cth) for a registered child sex offender to depart Australia without permission from the relevant State or Territory competent authority. A 'competent authority' is an entity with powers, functions or duties in relation to a child sex offender register – usually a State or Territory's court, sex offender registry or police service. The Act also authorised Australia's Minister for Foreign Affairs to deny a passport to a reportable offender upon request from a State or Territory competent authority.

In line with its legislated functions, which include assisting international law enforcement and crime prevention, the AFP may provide information relating to a registered offender's international travel to an international law enforcement authority. When notified, it is a matter for foreign law enforcement to determine what actions they take in relation to the offender, which may result in their entry to the country being prohibited.

The Department of Home Affairs manages alerts pertaining to reportable offenders through its border processing systems, ensuring that the AFP is notified when a registered offender attempts to depart Australia.

Treatment of Criminal Code offences under the Proceeds of Crime framework

In May 2021, the Government amended the *Proceeds of Crime Regulations 2019* to enhance law enforcement's ability to restrain and confiscate property that is the proceeds or an instrument of a child sexual abuse offence. Specifically, the amendments designated child sexual abuse offences in the *Criminal Code 1995* as 'serious offences' for the purpose of the *Proceeds of Crime Act 2002*. The effect of this is to enable the Australian Federal Police to restrain the property of persons who are reasonably suspected of having committed a child sexual abuse offence, and apply for it to be forfeited to the Commonwealth on the balance of probabilities. Crucially, these provisions enable non-conviction based asset confiscation, meaning that the person whose property is restrained and forfeited does not have to be convicted, or even charged, with an offence.

Child sexual abuse has clear links to transnational, serious and organised crime—sophisticated global networks are profiting from the sexual abuse of children, with low operating costs and high profits incentivising offenders. These offenders need assets to perpetuate their conduct, and grow their criminal businesses by reinvesting the proceeds of their offending to enable further, criminal conduct. By confiscating these assets, and the proceeds obtained from the offending, law enforcement is able to degrade the ability of these criminals to perpetrate further offending.

The electronic surveillance framework

The electronic surveillance framework provides law enforcement agencies with investigative tools to gather evidence of criminal activity, and other threats to the community, by accessing communications and other electronic data. This evidence is vital to their operations, including their investigation and prosecution of child exploitation, much of which is conducted in the online environment.

Telecommunications (Interception and Access) Act 1979 (TIA Act)

The TIA Act provides a legal framework for national security and law enforcement agencies to access information held by communications providers to investigate criminal offences and other activities that threaten the safety and security of Australians. The access that may be sought under the TIA Act includes access to telecommunications data, stored communications, and the interception of communications in real time.

Surveillance Devices Act 2004 (SD Act)

The SD Act authorises the use of surveillance devices by law enforcement agencies. The Act provides a single legislative regime for Commonwealth agencies to use surveillance devices (such as optical, listening, tracking and data surveillance devices) and a warrant framework to access data held in computers. The Act also authorises state and territory law enforcement agencies to use surveillance devices and access data held in computers under the Commonwealth regime in defined circumstances.

Other legislation which makes up the broader electronic surveillance framework includes the *Telecommunications Act 1997* which sets out how telecommunications are regulated in Australia and includes the industry assistance framework introduced by the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (TOLA). The *Crimes Act 1914* is also a part of the electronic surveillance framework, as TOLA inserted computer access warrants for law enforcement into this legislation.

The Government has also made a number of recent changes to enhance the framework. For example, the *Telecommunications Legislation Amendment (International Production Orders) Act 2021* which provides a framework for Australian agencies to obtain data directly from overseas communications providers where Australia has an agreement (such as an Australia-US CLOUD Act agreement). This is crucial to combatting online child exploitation, where Australian offenders use electronic services hosted, and with data stored, in other countries.

Future legislative reform

The Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 (SLAID Bill)

Increasingly, cybercrime is committed at volume, across multiple jurisdictions, using technology which anonymises the identity of offenders, and obscures visibility of content hosted on, and facilitated by, communications platforms. Current electronic surveillance powers are not suitably adapted to identifying and disrupting serious crime where criminals rely upon an ability to obfuscate their identities and illegal activities.

The SLAID Bill proposes to strengthen the capacity of Australia's federal law enforcement and criminal intelligence agencies—the AFP and the Australian Criminal Intelligence Commission (ACIC)—to identify and disrupt serious criminal activity occurring online, including child exploitation. The SLAID Bill introduces three new powers to enhance the ability of the AFP and the ACIC to keep pace with technological trends, and respond to serious cyber-enabled crime:

- data disruption warrants to enable the AFP and ACIC to access computers and modify data belonging to individuals suspected of criminal activity in order to frustrate the commission of serious offences online;
- network activity warrants to enable the AFP and the ACIC to access computers for the purpose of collecting intelligence on the most harmful criminal networks of individuals suspected of engaging in or facilitating criminal activity, including those on the dark web and using anonymising technologies; and
- account takeover warrants to enable the AFP and the ACIC to take control of a person's online account for the purposes of gathering evidence about criminal activity, to further a criminal investigation.

The SLAID Bill's disruption, intelligence collection and account takeover warrants will complement the AFP and the ACIC's existing powers by providing new avenues to gather information and respond to serious cyber-enabled crime, including child exploitation.

The PJCIS tabled its advisory report on the SLAID Bill on 5 August 2021. In its report, the PJCIS accepted that the threat from serious cyber-enabled crime is severe and Australian authorities do not currently have the tools to address the threat. The Government is carefully considering the Committee's recommendations, which went to tightening the use of powers and strengthening oversight and accountability.

Holistic reform of the electronic surveillance framework

As part of the Government Response to the Comprehensive Review of the Legal Framework of the National Intelligence Community (the Richardson Review) the Australian Government has established a dedicated taskforce to holistically reform Australia's electronic surveillance legislative framework. The reforms will repeal and replace the existing legislative framework currently divided between the TIA Act, the SD Act, and parts of the *Australian Security Intelligence Organisation Act 1979* with one consolidated Act. The reforms will modernise, streamline and future-proof the legislation underpinning law enforcement and intelligence agencies' access to electronic information to support their investigations, ensuring agency powers keep pace with technology.

Information and intelligence sharing

Information and intelligence sharing is crucial in the fight against child sexual exploitation and abuse, noting the borderless nature of this abhorrent crime. The below details a number of domestic information sharing mechanisms and further information on international arrangements can be found in the next section under **International Cooperation**.

Fintel Alliance

In 2017 the Fintel Alliance established a dedicated combating child exploitation project. This has significantly enhanced the value and application of financial intelligence to targeting and disrupting child exploitation in Australia and internationally.

The Fintel Alliance project has directly led to the arrest of individuals in Australia and the rescue of children from harm overseas. Highlighting the value of financial intelligence. Many of the individuals identified and arrested were not previously known to law enforcement.

Through bringing together government, law enforcement and leading financial institutions, Fintel Alliance has been able to increase the capability of financial institutions in Australia and internationally to detect and disrupt payments for child exploitation material.

The project identified avenues for public-private partnerships to achieve success through:

- bringing crime experts and representatives of financial institutions together to better identify opportunities for financial intelligence to influence investigations
- developing guidance and indicator information for financial institutions to enhance transaction monitoring and reporting suspicious behaviour
- using data analytical tools and keywords to identify activity for investigation
- matching data sets to develop more complete awareness of suspected offenders for targeting
- establishing relationships with partners in foreign countries and non-profit organisations, around an area of common focus.

In addition to achieving the aims of the project, opportunities were identified to increase the value of financial intelligence, through targeting child-like sex dolls and combining financial information with known offenders and facilitator lists.

When embraced by law enforcement, financial intelligence can play an important role in identifying unknown offenders operating in the community, and present opportunities for disruption.

National Child Offender System (NCOS)

The ACIC administers the National Child Offender System (NCOS) on behalf of State and Territory policing agencies. It is a web-based application that allows Australian police to record and share child sex offender information. It directly enables police in each state and territory to manage key information to meet their requirements under respective child protection legislation.

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.
- The **MPS** holds information on alleged offenders who are charged but not convicted, or after an offender's reporting obligations have been completed. The MPS supports the Australian Child Protection Offender Reporting scheme which has been established by legislation in each Australian state and territory. This national 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 period of time after they are released 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. The register and its supporting legislation also assists police in the investigation and prosecution of any future offences offenders may commit.

Potential improvements to the NCOS

The effectiveness of the NCOS as an information sharing mechanism could be leveraged by expanding access to Commonwealth law enforcement agencies: in particular, the ACIC and AUSTRAC.

While the ACIC administers the NCOS, it does not currently have access to the information or data contained within the system for intelligence or investigatory purposes. This significantly limits the ACIC's ability to work with the ACCCE and other agencies to develop a coordinated national intelligence picture of child sex offending, and to share relevant information and strategic insights with law enforcement partners.

By obtaining access to the NCOS, the ACIC would be able to undertake data analysis and matching against its criminal intelligence and national policing information holdings to:

- enhance 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 of resources to maximise disruption opportunities,
- generate additional insights about the child sexual abuse threat landscape, enabling the ACCCE and other partners to map, monitor and profile changes, and
- provide greater visibility to appropriate agencies undertaking prevention and interdiction activities, including national statistics about the number of registered child sex offenders in the NCOS and how these individuals are distributed across Australia.

If granted access to the NCOS, the ACIC could also leverage its specialist powers and tools, including coercive examinations and human source capabilities, to develop and disseminate strategic intelligence and break-through understandings of the methodologies, planning and motivations of child sex offender syndicates.

Additionally, AUSTRAC has recently played a growing role in combatting child sexual exploitation, which would be further enhanced by NCOS access. Since 2015 AUSTRAC has experienced a 945% increase in reporting of suspected financial transactions that relate to child abuse offending, which has supported law enforcement activities. Direct access to NCOS would significantly enhance and complement AUSTRAC's ability to detect child abuse through matching suspicious financial payments with offending, adding an extra layer of actionable intelligence. AUSTRAC would then be able to provide more targeted intelligence reports, monitor financial activity of registered offenders and assist with prioritisation of actionable intelligence.

Expanding NCOS access would require reforms to relevant State and Territory legislation.

AUSTRAC access to the National Police Record System (NPRS)

Our National Police Reference System (NPRS) enables Australian police agencies to share essential policing information with other police agencies.

It is specifically designed to equip operational police, anywhere in the country, with the knowledge they need to make on-the-spot decisions when dealing with persons of interest. It provides key reference data to support police officers, investigators and analysts. This includes important information about persons of interest to alert police about whether a person is likely to be dangerous or wanted for other offences.

The NPRS provides Australian police with detailed, current and accurate national police information that they can access from handheld devices, in-car terminals and desktop computers.

The system is available to more than 75,000 police officers across Australia. It provides access to more than 11 million records and 10 million photographs and records core data such as:

- name
- identity information and photographs
- information on warnings, warrants and wanted persons
- offence history
- protection and violence orders
- firearms involvements
- information relating to the child protection register
- information on missing persons, unidentified persons and bodies, and escapees.

AUSTRAC is seeking access to the ACIC-managed NPRS database to enhance AUSTRAC's financial intelligence. Direct access to the NPRS would expand AUSTRAC's capacity to efficiently respond to high-priority detection and disruption of child exploitation activities.

Enabling AUSTRAC access to the NPRS would require amendments to the Australian Crime Commission Regulations 2018, to make AUSTRAC a prescribed body.

Prospective initiative: the National Criminal Intelligence System (NCIS)

The National Criminal Intelligence System (NCIS) will be a whole of government capability, operating in a secure, national information sharing environment. It will support collation and sharing of criminal intelligence and information across state, territory and Commonwealth law enforcement.

NCIS will give Australia's law enforcement and intelligence agencies the first truly national, unified picture of criminal activity and enable police and law enforcement personnel to find the information they need to keep themselves and the community safe.

The Australian Government provided half of the funding to implement the first tranche of NCIS. The other half of the funding came from the National Policing Information Systems and Services Special Account. The initial build of NCIS, which began in 2018, will provide targeted, timely, relevant, prioritised national policing information, improving our ability to work together across jurisdictions and agencies.

NCIS will deliver:

- A secure and trusted information sharing platform across law enforcement.
- A national, unified view of law enforcement information from ACIC and law enforcement partners (including Commonwealth agencies).
- Services to enable ACIC partners to be aware when another agency is interested in an entity or person of interest to facilitate agency collaboration and enhance community safety and officer safety.
- Funding support for law enforcement partner agencies (excluding Commonwealth) to connect with NCIS to share and utilise national data.

NCIS actively involves multiple partners across state, territory and Commonwealth law enforcement and intelligence agencies in its development. Recent work with partners has prepared NCIS for real-world use by frontline operations.

Agencies will be progressively onboarded during 2021-22.

Currently NCIS contains a child protection register flag, based on National Police Reference System data. This flag indicates that a person of interest has been convicted of a relevant offence and has been placed on a state or territory child protection register.

AUSTRAC and Home Affairs joint profiling project

This project was developed by AUSTRAC and Home Affairs to identify and target travelling sex offenders, by monitoring transactional data to detect possible offending behaviours.

A person of interest (POI) was identified in one of the profiles, who previously had not come to the attention of law enforcement. Following AUSTRAC's referral, Home Affairs placed the POI on a watch list due to financial behaviour consistent with purchasing or accessing child exploitation material.

On 18 December 2019 the POI was arrested by the Australian Federal Police at Melbourne Airport and charged with possessing, controlling, producing, distributing or obtaining child abuse material outside Australia. The POI's occupation was stated as a School Principal, and he had been based in Singapore since August 2019. Prior to this role, the POI worked at international schools in China, Qatar and Kuwait.

AUSTRAC's intelligence contribution to the operation played a central role in the identification, targeting and interception of the POI. In addition, AUSTRAC analysis identified that the POI sent 170 small remittances totalling $29,689 to beneficiaries in the Philippines and Ghana over eight years (2011-2019).

International cooperation

Five Country Ministerial Forum

The Department works closely with partners through the Five Country Ministerial forum on a range of law enforcement challenges, including countering online child sexual exploitation and abuse.

In April 2021, Five Country Ministers agreed to a United Kingdom led feasibility study on a five country shared hash list, which could be used by law enforcement partners to identify child sexual abuse material online. The feasibility study will also consider whether the hash lists should be available to trusted, non-government organisations. The feasibility study is currently underway and the outcome will be shared at the next Five Country Ministerial Forum.

We work with international partners to identify policy or legislative developments that may impact the fight against online child sexual abuse, and seek to influence policy outcomes through our collective action. In December 2020, the European Electronic Communications Code (EECC) entered into application bringing with it a new definition of electronic communications services. As a result of this new definition, electronic communication services became subject to the 2002 ePrivacy Directive, which does not contain a legal basis for the voluntary detection of child sexual abuse material by online platforms using traditional methods.

In the 18 weeks after the EECC entered into force, the United States National Center for Missing and Exploited Children saw a 58% reduction in EU-related reports of child sexual abuse. In January 2021, Five Country Ministers issued a joint statement on the Temporary Derogation to the ePrivacy Directive to Combat Child Sexual Exploitation and Abuse. Five Country Ministers called on European Union partners to support the European Commission's proposed temporary derogation to the ePrivacy Directive, that would allow companies to continue using highly effective tools to detect, report and remove child sexual abuse material online.

The temporary derogation to the ePrivacy Directive was issued in April 2021, and allows service providers to continue to detect, remove and report child sexual abuse material and apply anti-grooming technologies until the end of 2022. Australia remains engaged on this issue through our five country partnership noting that the European Union committed to proposing overarching legislation to tackle child sexual abuse online in 2021.

On 5 March 2020, Five Country Ministers launched the Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse, which provide a high-level, best practice framework to guide online platforms and service providers to address the risk of online child sexual abuse. The Voluntary Principles were developed in partnership with digital industry (namely Facebook, Google, Microsoft, Roblox, Snap, TikTok and Twitter), non-government organisations and academia. Since then, we have secured 10 public endorsements of the Voluntary Principles and partnered with WeProtect Global Alliance to promote the Voluntary Principles to digital industry.

While the Voluntary Principles provide a critical framework to protect children online, and have encouraged industry to focus on safety as well as security, their voluntary nature and lack of transparent reporting mechanisms makes it impossible to measure their impact on combatting online harm. With the significant rise in reports of online child sexual abuse, it is clear that governments and industry need to do more. Despite continued collective pressure on digital industry to put safety at the forefront of their design, commercial interests continue to drive development decisions and emerging technology exposes more children to risk.

Other International and Digital Industry Engagement

Under the National Strategy to Prevent and Respond to Child Sexual Abuse, due to be announced later in 2021, the Department will deliver a package of measures aimed at enhancing digital industry engagement to combat online harms. As part of this package, the Department will position a Digital Industry Engagement Officer in the United States to spearhead direct engagement with technology companies, service providers, peak industry bodies and senior policy makers to garner greater support from industry to protect children online. An annual digital industry event will also be delivered that will focus on law enforcement solutions to emerging challenges for countering online child sexual abuse. Finally, a range of innovative communications products will be developed to shape the public narrative and stimulate informed debate.

Under the Strategy, the Department will also establish a Capacity Building team that will focus on working with our partners to strengthen criminal justice and law enforcement responses to child sexual abuse in the Indo-Pacific region.

In addition to this, we continue to work bilaterally with a range of international counterparts, sharing policy approaches and challenges to continue to elevate the issues of online child sexual exploitation and abuse and to build a coalition of like-minded governments to tackle this abhorrent crime.

International fora on childlike sex dolls

The Australian Border Force International Operations and Coordination and Investigations have hosted a number of international forums with the United Kingdom and New Zealand and soon with the United States to enhance the collaboration and cooperation of our global law enforcement partners.

This engagement has enabled greater international understanding of the risk posed by childlike sex dolls, distribution networks and supply chains. , investigation strategies and opportunities for law enforcement agencies to take a united approach to combat the risk posed by childlike sex dolls to protect communities across the globe.

Crossborder access to data

Technology has increasingly been a key facilitator of child sexual exploitation and abuse. Access to digital media and communications technologies is now a fundamental aspect of children's early ages, resulting in such technologies becoming thoroughly embedded in their lives. This, of course, significantly increases the opportunities for offenders to engage with, exploit and abuse, children.

While advances in technology have been a boon for offenders, they have also provided opportunity for law enforcement authorities to collect electronic data. This electronic data is often held by communications service providers that have customers all over the world. As such, access to this data is of increasingly high value to Australian law enforcement and national security agencies.

Communications service provider business models often involve offices and data storage facilities located in many different jurisdictions with some offering services in countries where they have no physical or legal presence. The nature of modern data storage systems and 'cloud computing' means that data is transient and can automatically move between physical international servers, making it challenging for law enforcement and national security agencies to identify where and by whom it is held. Further, this data is often deleted before law enforcement or national security agencies can obtain it.

Circumstances in which foreign communications service providers hold electronic data relevant to Australian criminal investigations and prosecutions often involve a complex web of legal compliance and regulation. What would traditionally have been an entirely domestic communication—between two people in Australia using a communications service offered to the Australian public—may now move through many different countries and may be subject to the laws of multiple countries restricting the disclosure of electronic data.

International crime cooperation

International crime cooperation mechanisms are crucial to obtain evidence, including electronic data, from foreign jurisdictions for use in criminal investigations and prosecutions. Australia's law enforcement agencies currently rely heavily on international crime cooperation mechanisms, such as mutual legal assistance, to access critical electronic data needed to combat serious crime, including child exploitation.

Despite heavy reliance, these existing cooperation mechanisms were designed before the internet and without considering the nature of modern telecommunications networks. Under the mutual legal assistance process, requests for communications data from foreign jurisdictions can take a significant amount of time. Due to the lengthy process associated with reviewing requests and engaging that country's investigatory powers to obtain information on behalf of the requesting country.

Alternatives to the mutual legal assistance process are also utilised to obtain electronic data from foreign jurisdictions, such as police to police and agency to agency assistance. However, these approaches can also be lengthy, and can result in information being provided that is not admissible in court due to the requirements of the *Foreign Evidence Act 1994*. Communications service providers also provide electronic data on a voluntary basis to law enforcement agencies, although this is not done by all providers in all circumstances and can therefore be an unreliable source of obtaining critical information for an investigation or prosecution.

Both the volatile nature of electronic data and the urgency to identify at-risk children require immediate action by law enforcement to not only prevent the loss of critical evidence, but to protect at-risk children from ongoing and repeated sexual exploitation and abuse. International crime cooperation is a major capability in Australia's law enforcement response to combating child sexual exploitation and abuse.

Case study: Delays in mutual assistance and prosecution of child exploitation

Delays in the current mutual legal assistance process can frustrate the successful investigation and prosecution of child exploitation offences.

In one case, an AFP investigation identified that child abuse material (CAM) was contained on an individual's devices, however specific content and data was not visible to law enforcement on the devices themselves as it was stored on the servers of carriage service providers in the United States and United Kingdom. The AFP ultimately received working copies of the evidence sought from one country after approximately 9 months. It was nearly 2 years before the AFP received information from the other country and, when received, the data was provided in a format which required extensive in-house resources and analysis to read.

In total, it took almost 3 years from the date of initiating the mutual assistance request process to receive working copies of the relevant material, with a further 18 months until receipt of the formally sealed MAR material. The delays faced in using the current processes not only frustrate the investigative process, but provide an opportunity for suspects to continue offending throughout that time, potentially resulting in further victims, and prolonging the trauma experienced by current known victims.

***Source:** Australian Federal Police Submission to the Parliamentary Joint Committee on Intelligence and Security (14 May 2020). Inquiry into the Telecommunications Legislation Amendment (International Production Orders) Bill 2020.*

The *Combatting child sexual abuse and exploitation through financial intelligence* report

An AUSTRAC-led international collaboration with the United Kingdom Financial Intelligence Unit and the Philippines' Anti-Money Laundering Council, resulted in the report *Combatting child sexual abuse and exploitation through financial intelligence*. The report was released in September 2020 by the Egmont Group of Financial Intelligence Units, and examines the role of financial intelligence in global efforts to fight online streaming of child sexual abuse and exploitation (CSAE).

The project team also comprised financial intelligence units from Canada, Denmark, France, Germany, Guatemala, Isle of Man, Indonesia, Latvia, Luxembourg, Malaysia, Mexico, the Netherlands, Nigeria, Norway, Peru, Seychelles and Interpol.

This work enhanced child protection and helped target abusers by increasing global understanding of the connection between financial flows and child sexual abuse. Money service businesses and payment service providers also provided input to the project, to increase mutual understanding of global risk indicators and improve suspicious matter reporting. The businesses involved were American Express, MoneyGram, PayPal, TransferWise, Western Union and WorldRemit.

The project team identified financial indicators, keywords and data sets that will be shared with law enforcement and industry to improve the identification and tracking of financial activity linked to online streaming of CSAE. Exploitation through live streaming means offenders can order, pay for and view children being abused anywhere in the world. Financial information is often a key component in fighting this horrific crime.

The project showed that financial intelligence and tactical collaboration is critical to combat CSAE. It also showed that integrating high-quality cyber-related data improved strategic and tactical intelligence, and allowed a more holistic picture to better combat CSAE globally.

Telecommunications Legislation Amendment (International Production Orders) Act 2021

The Government has undertaken significant work to modernise Australia's international crime cooperation frameworks, relationships and arrangements. In particular, the *Telecommunications Legislation Amendment (International Production Orders) Act 2021* (IPO Act), passed by Parliament on 24 June 2021, inserts the international production order framework into a new Schedule 1 to the TIA Act. This framework complements existing international crime cooperation mechanisms, such as mutual legal assistance.

Schedule 1 to the TIA Act sets out the legislative framework for Australia to give effect to future bilateral and multilateral agreements for cross-border access to electronic data for law enforcement and national security purposes. It will enable law enforcement and national security agencies to access electronic data in accordance with bilateral or multilateral agreements with foreign countries, by:

a. creating a framework for Commonwealth, state and territory agencies to obtain independently-authorised International Production Orders (IPOs) for data from designated communications providers in foreign countries (outgoing orders); and

b. permitting Australian carriers, carriage service providers and other relevant industry to disclose intercepted or stored communications data in response to incoming orders or requests from a foreign country (incoming orders).

In all cases, there must be a "designated international agreement" that has been assessed by the Attorney-General, in consultation with the Minister for Foreign Affairs and the Minister for Home Affairs, as meeting a range of statutory requirements (such as the foreign country respecting human rights and rule of law). Such agreements will be reserved for trusted partner countries noting that foreign law enforcement will be able to go directly to Australian communication service providers.

CLOUD Act Agreement being negotiated with the United States

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. The first agreement being considered for the IPO framework is currently being negotiated with the United States (commonly referred to as the 'AUS-US CLOUD Act Agreement'). Such an Agreement will streamline the process for obtaining electronic data in Australia and the United States by establishing a clear framework for direct cooperation between government agencies and communications service providers in both countries. Importantly, crucial evidence will be available sooner than is ordinarily the case when sought via mutual legal assistance when investigating, preventing, detecting, or prosecuting serious crimes such as child exploitation.

Budapest Convention and Second Additional Protocol

The Council of Europe Convention on Cybercrime (Budapest Convention) – which opened for signature in Budapest, Hungary, in November 2001 and came into force in 2004 – is the primary international crime cooperation treaty on cybercrime and the collection of electronic evidence. Australia acceded to the Budapest Convention on 30 November 2012, entering into force on 1 March 2013. The Budapest Convention provides member states with a framework on which to base their national legislation to criminalise cybercrime conduct, including offences related to 'child pornography' (noting Australia now refers to this as child abuse material) under Article 9 of the Convention, providing the necessary legal requirement for international cooperation on child abuse material under the Convention.

Budapest Convention Parties also have access to joint networks of practitioners to engage in trusted cooperation, for example, access to a 24/7 network of contact points to respond quickly and effectively to time critical requests: Australia's 24/7 network contact is the Australian Federal Police. Under the Convention, Parties are also able to improve their cooperation with the private sector (including direct cooperation requests) by building confidence and trust, as Parties need to have a domestic legal framework on cybercrime and electronic evidence in place, including the safeguards of Article 15. There are currently over 66 Parties to the Convention from around the world, with a further 11 countries invited to accede.

Since 2017, the Council of Europe Cybercrime Convention Committee (T-CY Committee) has been developing the *Second Additional Protocol on Enhanced Cooperation and Disclosure of Electronic Evidence* to the Budapest Convention. The Protocol the addresses the challenges posed by the impact of the digital age on crime and law enforcement by providing modernised measures for a more efficient international criminal justice response to cybercrime and crime involving electronic evidence. These measures include:

- provisions for streamlining and creating a more effective mutual legal assistance regime;
- provisions allowing for direct cooperation with communications service providers in other Party jurisdictions, subject to a strict set of limitations and safeguards; and
- more effective and secure trans-border access to data for Parties.

The Second Additional Protocol was developed by the Parties to the Budapest Convention (including Australia), ensuring the Protocol represents the diverse range of legal systems in the international community. The operative text of the Protocol and its Explanatory Report were finalised in May 2021 at the T-CY Committee level. The Protocol is likely to open for adoption in November 2021 and for signature in mid-2022. It will be a matter for the Australian Government to determine whether Australia will sign up to the Second Additional Protocol.

The International Statement: end-to-end encryption and public safety

The *International Statement: end-to-end encryption and public safety,* signed by seven countries, including Australia, and released in October 2020, calls on technology companies to work with governments to find mutually agreeable solutions to the issue of lawful access and public safety. Technology companies have an important role to play in preventing child abuse online and proactively reporting and engaging with law enforcement. (See **Lawful access and End-to-end encryption** in the next section for further information).

The role of technology providers

Technology providers have a responsibility to assist law enforcement agencies in investigations into child exploitation. Child exploitation is increasingly carried out online, utilising the services and platforms of these providers. The assistance of technology providers is critical for law enforcement agencies to identify and investigate these crimes, and reduce harm to victims. This is particularly the case as more and more providers adopt end-to-end encryption, and other anonymising technologies. These technologies limit the effectiveness of traditional law enforcement tools, such as interception.

Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (TOLA)

The widespread adoption of encryption hinders the utility of traditional electronic surveillance powers, such as interception warrants, to gather intelligible information.

Given the globalised, multi-layered nature of this industry, the range of entities with the capability to assist is diverse and expansive. Many providers are based offshore.

The TOLA introduced a new industry assistance framework—a framework for national security and law enforcement agencies to work with designated communications providers (DCPs), including in the execution of a warrant. The concept of DCPs captures entities across the full communications supply chain, reflecting the broad range of bodies that may meaningfully assist agencies. This includes providers based offshore who offer services in Australia. Agencies may only seek this assistance from DCPs to perform their functions or powers as conferred by or under law, so far as the function or power relates to a relevant objective. The assistance DCPs provide is intended to strengthen the ability of agencies to investigate crime in the new digital era.

The assistance framework cannot be used to ask providers to build a systemic weakness or vulnerability into a form of electronic protection. This includes actions which would make systemic methods of authentication or encryption less effective.

Since TOLA came into force on 9 December 2018, the industry assistance framework has been used in a targeted and cooperative manner to resolve technical issues hindering the investigation of a range of serious crimes. The industry assistance framework complements other tools available to law enforcement agencies to combat child exploitation.

TOLA also introduced computer access warrants to enhance the ability of law enforcement to access evidence on a device where it is unencrypted. Computer access warrants authorise direct access (including remote access) to a device for the purpose of gathering evidence.
TOLA is currently subject to review by the PJCIS.

Lawful access and End-to-end encryption

Lawful access refers to the limited circumstances in which law enforcement and intelligence agencies require proportionate access to online communications and other content from technology companies under formal requests for assistance, including under warrant. There are robust safeguards and strict oversight mechanisms that ensure agencies gain access to this information with legality and propriety.

The Australian Government acknowledges that strong encryption plays a crucial role in keeping all Australians safe online. However, there are online environments – such as on social media and social media messaging platforms – in which this level of encryption presents significant public safety risks, especially to children.

The normalisation of anonymising technologies like end-to-end encryption by digital platforms - including on social media - is bringing Dark Web functionality to the mainstream. Despite the well-founded concerns of Governments, law enforcement agencies and non-government organisations in relation to these technologies, large digital industry players continue to use prolific encryption in the name of privacy, creating obstacles for law enforcement in investigating serious crime, and making it easier for offenders to perpetrate serious abuse without detection. This is the case across all crime types but is particularly salient in cases of child sexual exploitation and abuse. The increasing use of anonymising technologies will be detrimental to all efforts to counter online child sexual exploitation and abuse; prevention, mitigation, victim identification, and perpetrator accountability.

Child sex offenders' use of encrypted technologies on social media platforms is enabling them to groom their victims knowing that they can do so without law enforcement being able to access the content of their communications, even in those instances in which police have a reasonable suspicion that offences are occurring. Large social media platforms provide a forum for these criminals to connect, share and trade tactics, as well as images of victims.

The recent passage of Australia's Online Safety Act, and Telecommunications Legislation Amendment (International Production Orders) Act 2021 are positive steps, and will facilitate greater takedown powers for eSafety, and smoother international law enforcement processes respectively.

Some social media and communication platforms, including Facebook, currently utilise proactive tools to detect child sexual abuse material (CSAM), and report incidents of CSAM to the United States National Centre for Missing and Exploited Children (NCMEC).

- In 2020, the NCMEC's CyberTipline received more than 21.7 million reports of apparent CSAM, including 65.4 million videos, images and files. This is an increase of 28 per cent from 2019.
- In 2020, Facebook made 20.3 million (93%) of the total 21.7 million total reports to the NCMEC. Following triage, the NCMEC referred 21,148 reports to Australian law enforcement.

Digital Industry should adopt Safety-by-Design (SbD) principles across its technologies and services, in accordance with the message in the *International Statement: End-to-End Encryption and Public Safety*. This would enable law enforcement access to content in a readable and usable format where an authorisation is lawfully issued, is necessary, proportionate, and is subject to strong safeguards and oversight.

Relationship between online and contact offending

When examining the relationship between online and offline offending, an important question to ask is whether online offenders are different to contact sexual offenders. A meta-analysis of 30 studies, comparing CSAM-only offenders with contact offenders against children and 'dual offenders' (those who committed both CSAM and contact offences) 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 (Babshishin, Hanson and VanZuylen 2015). An Australian study compared CSAM offenders with contact sexual offenders against children and dual offenders, finding 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. 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 (Henshaw, Ogloff & Clough 2018).

What proportion of CSAM offenders 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 had a *previous* contact sexual offence conviction at time of their online offence.

Where *reoffending* is concerned, re-analysis of systematic review data gathered by Dowling et al. (2021) 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.

Self-reported contact sexual offences by CSAM offenders tend to be higher. 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.

Online grooming leading to other forms of child abuse offending

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. 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).

Live online child sexual abuse

Live online 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). 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).

Because CSA live streaming offenders communicate and form relationships with victims and facilitators online (Teunissen & Napier forthcoming) (unlike with most CSAM viewing), they may be at risk of travelling to offend in person against these children or other children (Europol 2019).

Conclusion

The Department of Home Affairs is advancing efforts to combat child sexual exploitation and abuse through a range of activities including through legislative reforms and enhancing criminal justice responses, facilitating law enforcement cooperation, digital industry engagement and working with our international partners to build a coalition of like-minded governments to tackle this abhorrent crime.

To build on these existing efforts, the Home Affairs Portfolio has received over $80 million in funding in the 2021-22 Federal Budget to lead initiatives under the first *National Strategy to Prevent and Respond to Child Sexual Abuse,* soon to be launched by the Australian Government. These initiatives will bolster Australia's law enforcement, intelligence and criminal justice responses to child sexual abuse, and include the following:

- An additional $63.8 million provided to the Australian Federal Police across four years providing a significant capability uplift to child protection frontline efforts including victim identification, technology support to support police and specialist users, and additional capacity to target the organised crime aspects of online child sexual abuse.,
- $11.9 million over four years to enhance Australia's capacity to detect, disrupt and investigate child sex offending online and at the Australian border, boosting the intelligence, enforcement and research capabilities of AUSTRAC, the Australian Institute of Criminology, the Australian Criminal Intelligence Commission, the Australian Border Force and the Department of Home Affairs,
- $3.9 million to uplift the AFP's contribution to the Republic of the Philippine's law enforcement efforts to combat live online child sexual abuse,
- $4.1 million for the Department of Home Affairs to support our partners in the Indo-Pacific region to strengthen their criminal justice response to child sex offending, and
- $2.95 million for the Department of Home Affairs to build relationships with digital industry, driving a coordinated and collaborative charge against offenders' use of online platforms to engage in child sexual abuse.

The rapid development of anonymising technologies like end-to-end encryption has brought dark web capability to the clear net, and created a safe haven for offenders beyond the reach of law enforcement.

Home Affairs continues to strive to ensure criminal justice and law enforcement responses are maintained in step with complex and challenging technological advancements.

Australian Government

Department of Home Affairs

Department of Home Affairs supplementary submission to the Inquiry into law enforcement capabilities in relation to child exploitation

Parliamentary Joint Committee on Law Enforcement

12 January 2022

Table of Contents

Overview

The Department of Home Affairs (the Department) provided a written submission to the Inquiry on 3 September 2021 and appeared at a public hearing on 10 December 2021. The purpose of this supplementary submission is to provide additional context to the statements made by witnesses at the public hearings on 9-10 December 2021, as the Department was not provided with an opportunity to address these as part of its appearance before the PJCLE.

Balancing privacy, safety and security, and the rights of children

Cyber security tools, such as encryption, play an important role in keeping us safe online and protecting user privacy. However, it is essential that we balance protecting individual user privacy with other threats to public safety online. This is particularly important with respect to platforms that are used by children and adolescents, and also exploited by perpetrators of child sexual abuse crimes.

The Department remains deeply concerned that some digital platforms are using encryption tools to the detriment of public safety. Despite Meta's evidence to the Committee on 10 December 2021 that they are looking to balance privacy and safety, the Department's engagements with Meta and other companies with 'privacy first' polices reveal seeming indifference to public safety imperatives, including in relation to child safety.

To illustrate this, in the case of Facebook Messenger end-to-end encryption will only apply to the content of messages, which is of little commercial value to the company. The Department understands that personal data, such as metadata and site and cookie tracking, could still be exploited by Meta for commercial purposes, in line with their business model. For this reason, we welcome the Committee's scrutiny of Meta's claim that:

> *"…when things are end-to-end encrypted, that limits our ability to access additional data for the tightening of ads, so it's certainly not in our commercial interest, in this sense. This is primarily consumer driven."* (Mia Garlick, 10 December, Public Hearings for the PJCLE inquiry into law enforcement capabilities in relation to child exploitation)

While the Department welcomes Meta's acknowledgement of the need to balance privacy and safety, we are yet to see tangible evidence of how they intend to embed safety into their platform design. We remain unconvinced that their current plans to adopt end-to-end encryption will not be detrimental to the ability to keep children safe from online child sexual abuse.

Technical solutions to allow for the detection of child sexual abuse material (CSAM) in an end-to-end encrypted environment

Debate on end-to-end encryption has become increasingly polarised, and some privacy advocates argue that, in the application of end-to-end encryption, it is all or nothing. We reject this. It has been demonstrated that it is possible to develop tools that allow scanning for CSAM in a fully end-to-end encrypted environment, without impeding on a user's privacy.

For example, on 6 August 2021, Apple announced the rollout of a new feature called 'NeuralHash', which allows on-device scanning of images to detect CSAM on iOS devices. The new feature will reportedly detect a hash match against a database of known child abuse imagery before an image is uploaded to iCloud Photos, within an end-to-end encrypted ecosystem. Child sexual abuse material that is detected will then be referred to the US-based National Center for Missing and Exploited Children (NCMEC) for triage and investigation. Unfortunately the announcement from Apple was met with significant backlash from privacy advocates, and it is now unclear if Apple will implement this technology as previously intended.

The Department continues to encourage industry, including Meta, to identify technical solutions that better balance privacy and safety. Industry must invest in proactive safety technologies for their platforms, and platforms should be designed from the beginning to prevent and detect misuse.

Artificial intelligence and machine learning as tools to detect child sexual abuse material

Meta provided testimony that they use and continue to develop tools such as artificial intelligence and machine learning, intended to detect problematic behaviour signals. Despite repeated requests, the Department has not been provided with any verifiable evidence to suggest that these tools are effective. Further, despite repeated requests, the Department has not been provided with any examples of what a CSAM referral to NCMEC may look like following the implementation of end-to-end encryption. This means the Department is not able to determine if reporting will contain sufficient information in the form of indicators to facilitate further law enforcement investigations.

The Department is also concerned that once Messenger and Instagram Direct move to default end-to-end encryption, the artificial intelligence and machine learning tools will no longer be able to detect and learn from new content, meaning their effectiveness would diminish rapidly

Victim-dependent reporting is an ineffective and inappropriate model

Meta has indicated that following the implementation of end-to-end encryption on Messenger and Instagram Direct, there will be a significant dependence on victim reporting. Law enforcement will also rely more heavily on victims having to screen shot or capture images, videos or chat logs as evidence of an offence.

Placing the onus on victims to report abuse will mean law enforcement can only respond to victims where abuse has already taken place, and the consequent harms have been realised. While secondary intervention approaches are important in addressing abuse and protecting at risk children from further exploitation, primary prevention strategies are key to preventing long-term harms, and addressing the underlying causes of child sexual exploitation and abuse.

Australian research suggests that a significant proportion of CSAM is produced and distributed by parents who victimise their children, with 90% of offenders being men and victims being predominately girls under nine years of age[1]. Parental offenders exert greater control and have more access to their victims than extra-familial or online offenders. Victims of parental abuse are the least likely group to disclose their abuse, posing grave challenges for victim reporting and identification. Embedding safety by design into platforms and harnessing innovative risk assessment tools to target both victims and offenders will support deterring and protecting vulnerable cohorts of children.

Special consideration should be given to ensuring risks unique to children are adequately managed. These include content risks (which generally position the child as a recipient of unwelcome or inappropriate content), contact risks (where a child participates in risky communication, unwittingly or unwillingly), and conduct risks (where a child's behaviour contributes to risky content or contact within a wider peer-to-peer or adult-to-child network). As such, platforms that have a large number of users who are children or under the age of 18 should not adopt reporting models that predominantly rely on victims self-reporting.

In light of the continued moves by Meta and other platforms to deploy end-to-end encryption, the Department is exploring what policy or regulatory measures may operate to ensure appropriate safety measures are adopted.

Algorithmic promotion and persuasive technologies

The increasing ubiquity of the internet in our daily lives has magnified the potential harms of persuasive technologies, which are specifically designed to change or shape a user's behaviour. Digital industry's financial interest in attracting and retaining users has resulted in the implementation of algorithmic promotion of material and persuasive designs in their platforms.

Algorithmic persuasion is a means of encouraging and increasing a user's engagement with a particular platform by using big data and machine learning to analyse individual and broader user interaction, and "feed" the user content that is likely to gain their attention (filter bubble). This can result in digital echo chambers, where users are shown the same information, and encouraged to interact or join groups of people who share the same viewpoints, while differing opinions or information is not brought to their attention.

While human behaviour inclines people to group together in this way, the accessibility and ease of amplifying and spreading opinions via digital platforms increases the reach and speed at which divisive or abhorrent content can spread, fuelling racism, violence, and extreme political views.

The Department has significant concerns about the far-reaching consequences that persuasive design and algorithms have for both the individual user, and society more broadly. In particular, the impacts on children and vulnerable people, health and safety, the control of information, market dominance, the proliferation of misinformation and disinformation, and the creation of echo chambers and filter bubbles where content is siloed and extreme views are amplified (including those of perpetrators of child sexual abuse offences). The fact that platforms are actively selecting and promoting content using an algorithm raises questions about whether they are acting as publishers and should be regulated as such.

The Department is exploring potential policy or regulatory responses to these issues and is currently in the process of determining immediate research needs, in close collaboration with the Department of Infrastructure, Transport, Regional Development and Communications.

[1] Production and distribution of child sexual abuse material by parental figures | Australian Institute of Criminology (aic.gov.au)

Australian Government
Department of Home Affairs

Home Affairs intelligence led data based border targeting achieves significant border outcomes and generates significant investigative opportunities

Background

In 2018, the Department of Home Affairs Intelligence Division initiated a project to discover previously unknown travelling child sexual exploitation offenders and those carrying child abuse material (CAM) across the border. Targets identified in this project are generally not identifiable through traditional intelligence analysis or existing border targeting.

The Australian border presents a unique environment for targeting, intervention and collection. This environment is one characterised by unique datasets, specialist intervention and questioning powers and capabilities, and the evidenced ability to not only generate border detections, but also provide valuable operational leads for investigation.

By combining unique Home Affairs data with Australian Border Force (ABF) intervention powers, and applying sophisticated threat discovery capabilities such as data profiling, Intelligence Division's collaboration with the Fintel Alliance and AUSTRAC has successfully merged financial analysis with intelligence-led data based border targeting to achieve results. This has achieved significant results in countering child exploitation.

Outcomes

Home Affairs Intelligence Division has contributed to the detection of child abuse material at the border, identified post border investigation opportunities and facilitated discovery of previously unknown travelling child sex offenders.

Overview of outcomes
Intelligence Division's approach and collaboration with Australian Border Force (ABF) partners has generated:

- 62 CAM detections at the border;
- 24 detections of other material, frequently borderline CAM;
- A significant number of referrals for investigation; and
- Large amounts of information and derogatory intelligence collected revealing activities of previously unknown child exploitation targets.

These outcomes have created opportunity for post border activity directly leading to:

- 27 arrests by investigative partners in the ABF or Australian Federal Police (AFP) Joint Anti Child Exploitation Teams (JACET);
- 23 facilitators arrested overseas, with the identification of a further 17, from JACET investigations and AFP activity; and
- 72 children rescued or removed from harm, with the identification of a further 68, also from JACET investigations and AFP activity.

Notably, since international travel re-commenced in early 2022, 31 significant events have occurred as a result of the Home Affairs Intelligence Division and AUSTRAC data profile, with 17 targets being detected with CAM at the border, nine of which were subsequently arrested.

Case Study A:

- On 25 October 2019, a 56-year-old Australian male was detected with CAM at the border. The male had not come to the attention of law enforcement for child exploitation activity or suspicion and was targeted as a result of a Home Affairs Intelligence Division and AUSTRAC data profile.

- A subsequent JACET investigation resulted in:
  - The male being charged with over 75 offences;
  - Three facilitators arrested overseas, with a further 17 identified;
  - Seven children rescued or removed from harm overseas, with a further 52 identified; and
  - https://www.afp.gov.au/news-media/media-releases/queensland-man-charged-alleged-online-sexual-abuse-50-philippines-children.

Case study B.

- On 28 February 2020, a 66-year-old Australian male was detected with CAM at the border. The male had not come to the attention of law enforcement for child exploitation activity or suspicion, and was targeted as a result of a Home Affairs intelligence Division and AUSTRAC data profile.

- A subsequent JACET investigation resulted in:
  - The male pleading guilty to 50 offences, which included charges relating to viewing, remotely instructing and recording the sexual abuse of children on 55 occasions between March 2018 and January 2020;
  - Five facilitators arrested overseas;
  - 15 children rescued or removed from harm overseas, with a further 52 identified; and
  - The identified male was sentenced to more than 15 years' imprisonment.

Update to outcome in previous submission

The previous submission detailed the case of a 58-Year-old Australian male through the following dot points:

- A person of interest (POI) was identified in one of the profiles, who previously had not come to the attention of law enforcement. Following AUSTRAC's referral, Home Affairs placed the POI on a watch list due to financial behaviour consistent with purchasing or accessing child exploitation material.

- On 18 December 2019 the POI was arrested by the Australian Federal Police at Melbourne Airport and charged with possessing, controlling, producing, distributing or obtaining child abuse material outside Australia.

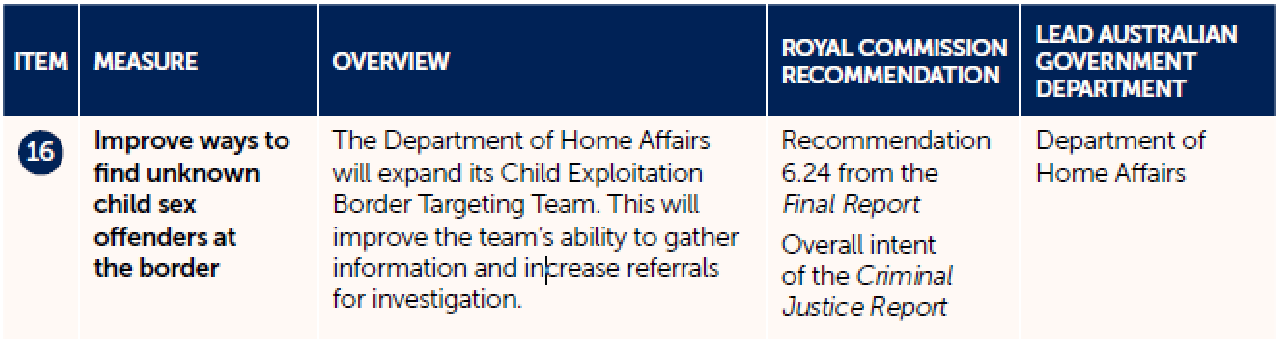
- The POI's occupation was stated as a School Principal, and he had been based in Singapore since August 2019. Prior to this role, the POI worked at international schools in China, Qatar and Kuwait.

A JACET investigation has progressed since the last submission, with the POI pleading guilty to 13 charges and sentenced to five years gaol, with a non-parole period of three years. The POI will be a registered offender for life.

Current and future development

Intelligence Division continues to contribute to operational successes combatting child abuse through improved analytical tradecraft and close collaboration with a range of intelligence, operational and policy partners.

This contribution is reflected in the National Strategy to Prevent and Respond to Child Sexual Abuse and First Commonwealth Action Plan to Prevent and Respond to Child Sexual Abuse 2021–2024, specifically Theme 4: Offender Prevention and Intervention item 16:



ITEM	MEASURE	OVERVIEW	ROYAL COMMISSION RECOMMENDATION	LEAD AUSTRALIAN GOVERNMENT DEPARTMENT
16	**Improve ways to find unknown child sex offenders at the border**	The Department of Home Affairs will expand its Child Exploitation Border Targeting Team. This will improve the team's ability to gather information and increase referrals for investigation.	Recommendation 6.24 from the *Final Report* Overall intent of the *Criminal Justice Report*	Department of Home Affairs

Intelligence Division has increased border targeting of child-like sex dolls through dedicated collaboration with Five-Eyes border partners and private industry, and utilisation of online and non-traditional data sources. This has already resulted in significant outcomes and the protection of children. For example:

- In January 2021, an Intelligence Division border profile identified an air cargo consignment suspected of containing a child-like sex doll and destined for a 61-year-old Australian male in regional NSW. Subsequent collection, analysis and referral of high-risk online activity and purchase behaviour resulted in search and seizure warrants and the arrest of the intended recipient of the consignment.
- The 61-year-old male was recently gaoled for five years for importing a child-sex doll and installing cameras in a 12-year-old child's bedroom.
- https://www.dailyliberal.com.au/story/7925256/shocked-and-betrayed-coonamble-man-caught-with-child-abuse-material-and-child-sex-doll-remains-behind-bars/

Home Affairs Intelligence Analysts have been embedded in the AFP-led Australian Centre to Counter Child Exploitation (ACCCE) to contribute to and support ACCCE functions and priorities:

- Collaboration between the ACCCE and Home Affairs Intelligence Division to utilise existing data sets for border targeting has resulted in 11 detections of CAM at the border since mid-2022. These detection outcomes and other activity occurred in relation to targets not identifiable through traditional methods or under current prioritisation.

Further collaboration and lines of effort by Intelligence Division are underway to utilise analytical tradecraft, knowledge and data to match, prioritise, assess and refer child exploitation where targets do not interact with the Australian border, or targets seek to gain access to children for sexual exploitation through migration and citizenship pathways.

Ongoing and future challenges

Information sharing, technology and border intervention response capability and capacity are the main challenges to the ongoing and future success on Home Affairs Intelligence Division's child exploitation targeting project:

- The precision and efficiency of current data profiles, as well as the speed at which new financially themed profiles can be developed is limited by data sharing restrictions between AUSTRAC and Home Affairs. This results in the inability to develop and deploy fully automated data based profiles across combined live data sets of AUSTRAC (financial) and Home Affairs (travel, cargo, visa, citizenship).

- ABF technical capabilities and infrastructure to detect CAM on mobile devices is crucial, but limited by various factors. The size and storage capacity of modern devices, combined with the speed of IT software and hardware used to assess content makes this problematic.
- ABF resources, training and capabilities have limitations. National inconsistency in approach and achievement of outcomes are evident and limit operational outcomes.

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.

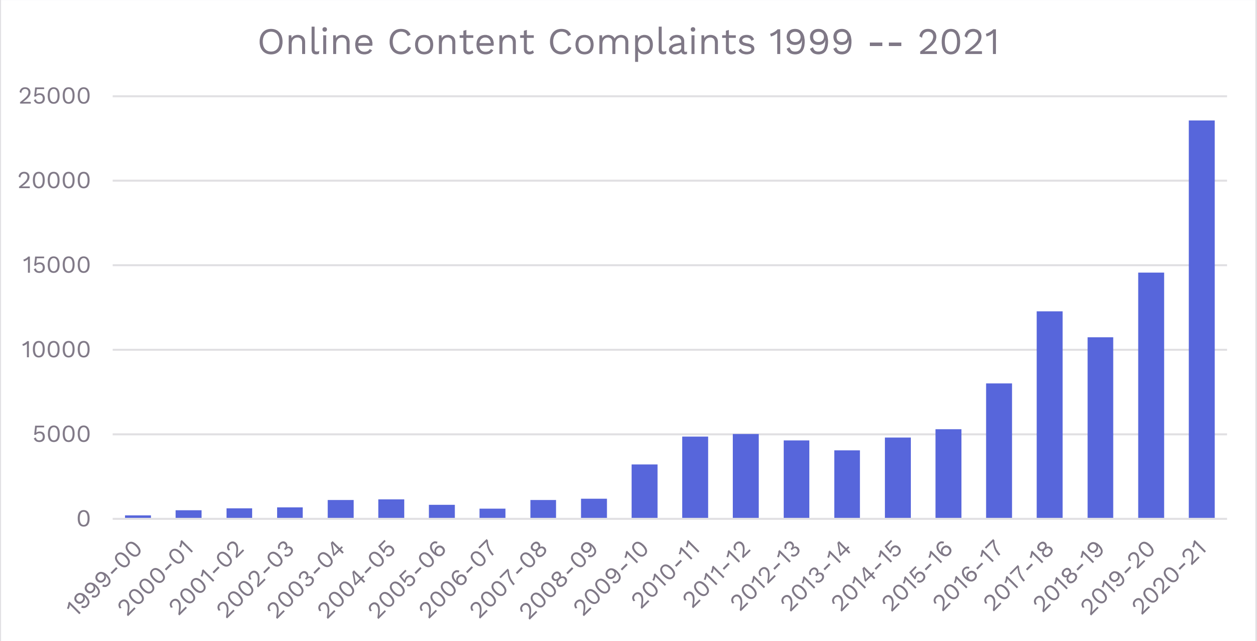
The Canadian Centre for Child Protection (C3P) has, through its Arachnid program,[3] detected and verified more than 5.4 million child sexual abuse images since 2018. Through the program, C3P has notified more than 760 electronic service providers worldwide that they are hosting CSEM. Almost 85% of the 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.

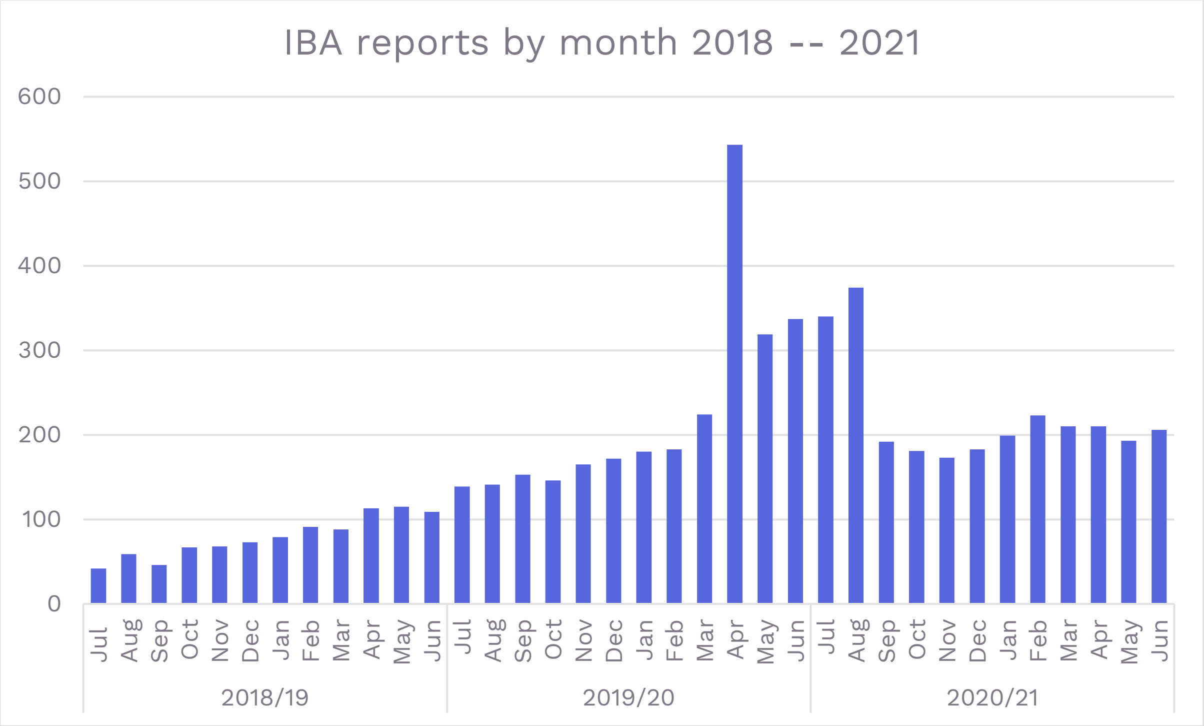
We might also:

- 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.

Australian Government | eSafetyCommissioner

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:

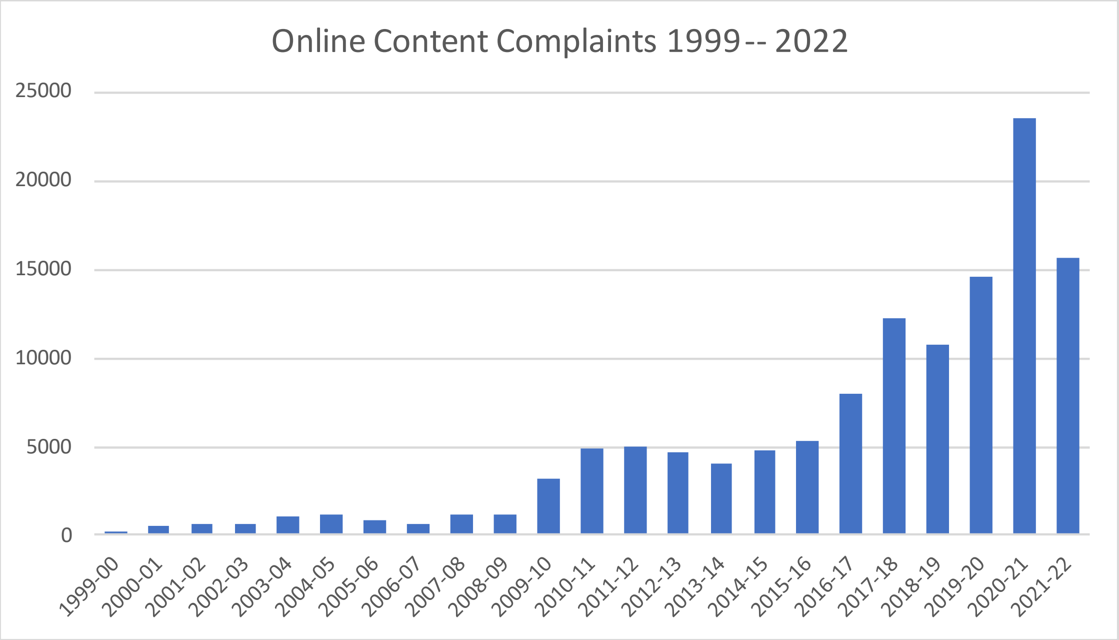
- develop and drive a global coordinated response to child sexual abuse online
- secure engagement at national, regional, and global levels
- showcase progress and champion best / emerging practice
- influence and contribute to key WeProtect Global Alliance products and membership commitments.

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.

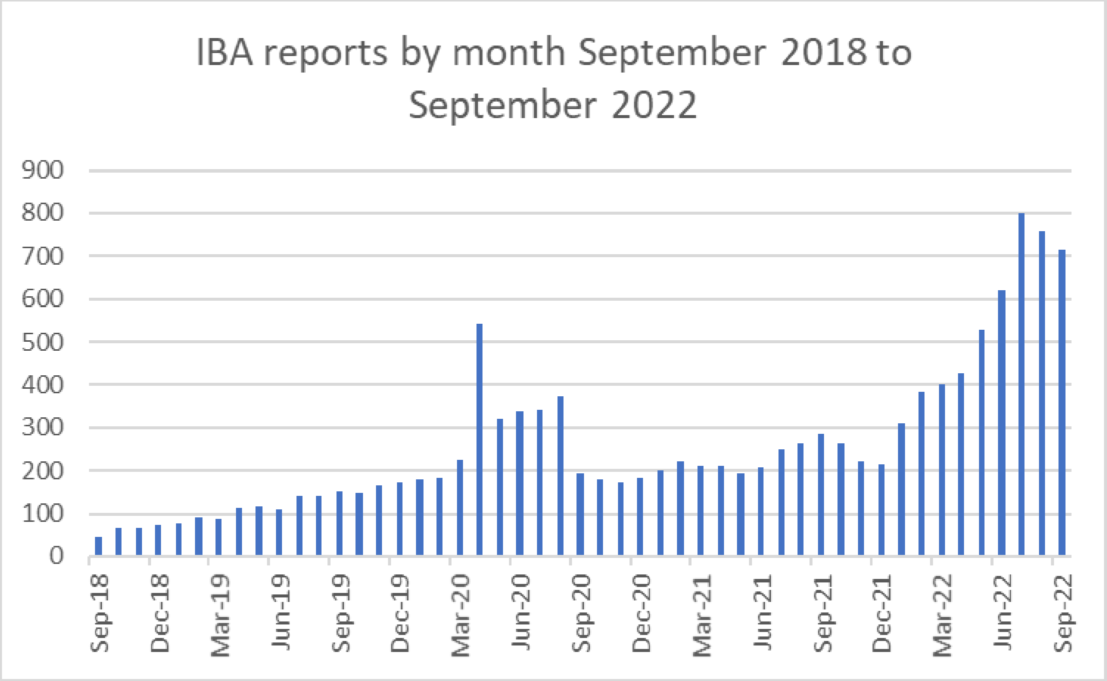
We may also:

- 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.