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:

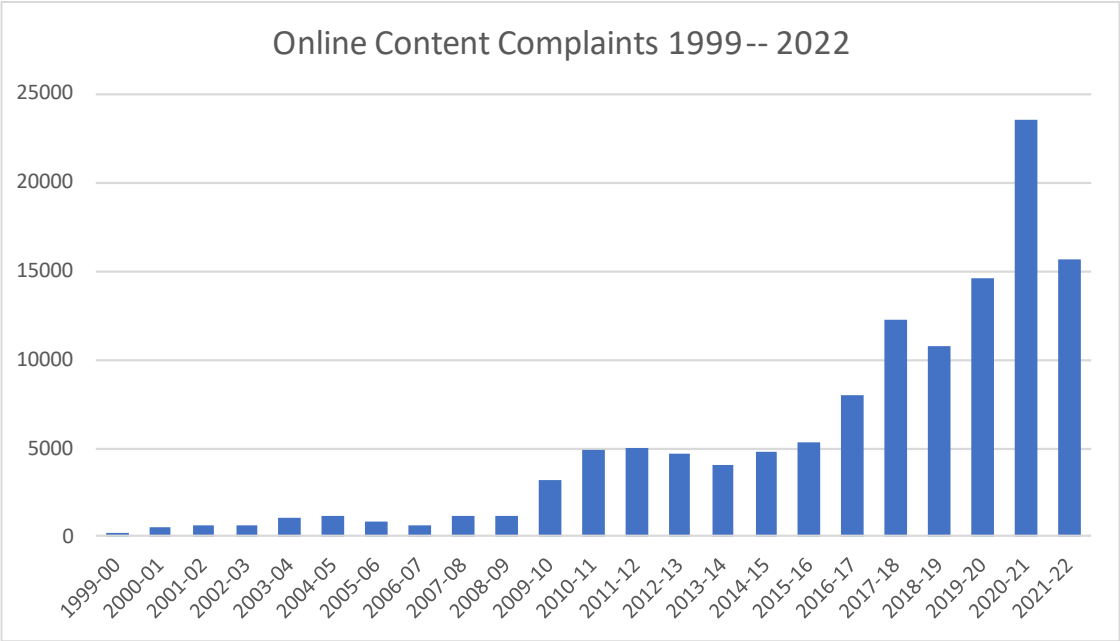
- develop and drive a global coordinated response to child sexual abuse online
- secure engagement at national, regional, and global levels
- showcase progress and champion best / emerging practice
- influence and contribute to key WeProtect Global Alliance products and membership commitments.

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.

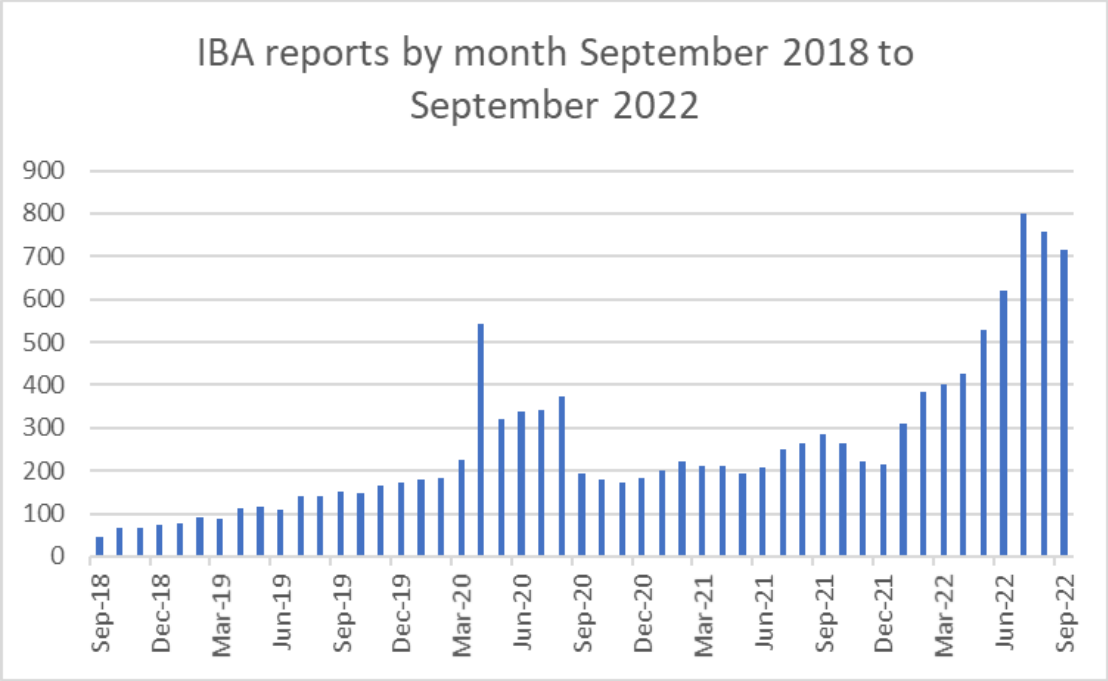
We may also:

- 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.