CYBER SECURITY
COOPERATIVE
RESEARCH
CENTRE

CSCRC SUBMISSION: Law enforcement capabilities in relation to child exploitation

cybersecuritycrc.org.au

Dear Sir/Madam,

Submission: Law enforcement capabilities in relation to child exploitation

The Cyber Security Cooperative Research Centre (CSCRC) is pleased to make this submission to the Parliamentary Joint Committee on Law Enforcement's inquiry into *Law enforcement capabilities in relation to child exploitation.* This inquiry is particularly timely given the exponential increase in the production and distribution of child abuse material (CAM) , which has been fuelled by the COVID-19 pandemic. It is essential Australia remains a prosperous, digital nation while also protecting the most vulnerable members of our community – our children – from online sexual exploitation.

About the CSCRC

The CSCRC is dedicated to fostering the next generation of Australian cyber security talent, developing innovative projects to strengthen our nation's cyber security capabilities. We build effective collaborations between industry, government and researchers, creating real-world solutions for pressing cyber-related problems.

By identifying, funding and supporting research projects that build Australia's cyber security capacity, strengthen the cyber security of Australian businesses and address policy and legislative issues across the cyber spectrum, the CSCRC is a key player in the nation's cyber ecosystem. The CSCRC has two research programs: Critical Infrastructure Security and Cyber Security as a Service.

We look forward to answering any queries regarding this submission and welcome the opportunity to participate in future discussions on this very important topic.

Yours Sincerely,

Rachael Falk
CEO, Cyber Security Cooperative Research Centre

Introduction

Sexual offences against children are among the most abhorrent crimes that occur in our society – whether committed online or offline. Before the advent of the internet, these crimes generally occurred when an offender could access child victims. However, the proliferation of the internet and encrypted messaging applications has proven a boon for child sexual offending and the production and distribution of child abuse material (CAM). While there are perceptions the victims of these crimes are overwhelmingly located in overseas jurisdictions, many are also Australian. And the methods used by their abusers grown ever-more sophisticated, with encrypted apps and the dark web providing a "cloak of invisibility"[1] to their offending.

Accessing and viewing CAM is not a victimless crime, as many perpetrators believe.[2] It has a devastating and lifelong impact on the children that are abused, with abuse images living on unfettered in the uncensored world of clandestine online CAM groups. And, unfortunately, Australians are some of the most prolific consumers of this material, with research indicating Australia is the third largest market for live, online child sexual abuse.[3] Likewise, the average number of images police seize from offenders has exploded – in the early to mid-2000s, offenders averaged about 1000 images; now it is 10,000 to 80,000 images and videos.[4]

Given the scale of CAM and the devastating impacts it has on the millions of exploited child victims around the world every year, it is necessary that law enforcement has appropriate powers to detect, disrupt and bring offenders to justice. To this end, the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020*, which is currently before Federal Parliament, will, if passed, be a game-changer in tackling the scourge of CAM. However, this is a shared responsibility and there is a clear role for technology providers to help law enforcement combat CAM through monitoring, removal and reporting of such content.

Finally, the CSCRC submits that an absolute right to privacy can never exist and there must always be exceptions, especially when it comes to maintaining the common good. This is a principle recognised in the International Convention of Civil and Political Rights, which

---

[1] Commissioner Reece Kershaw APM - National Child Protection Week | Australian Federal Police (afp.gov.au)
[2] 0066_Harm, prog and addiction A4_v4.pdf (accce.gov.au)
[3] Explosion of online child abuse shames Australia, but we must talk about it (theaustralian.com.au)
[4] Ibid 3

makes explicit exceptions where privacy can be overridden, including for the protection of national security, public order, or of public health and morals.[5]

The CSCRC contends that while privacy is valuable it must have limitations and these limitations must correlate with the social contract all members of the community enter into, upon which modern democracies like Australia's are built. Social contract theory holds that for society to function properly individuals must give up certain rights. This is a concept that can no longer simply be applied to the physical world – in 2021, it must also incorporate unacceptable behaviour that occurs in the digital domain.

Trends and changes in relation to the crime of online child exploitation

Electronic communications via the internet, mobile phones and the advent of numerous encrypted communication platforms have undoubtedly increased the prevalence and volume of CAM, allowing horrific and depraved images of child abuse to be beamed across the world with the press of a button. And, though widespread prior to COVID-19, the pandemic has created the perfect environment for the spread of online CAM to become ever more pervasive.

A recent United Nations report found COVID-19 has increased and accelerated the sexual exploitation of the some of the world's most vulnerable children, "amplifying the risks of exposing them to sale, trafficking and sexual exploitation globally".[6] The report notes the pandemic and an increased use of online platforms has increased unsupervised time spent on the internet, exacerbating already existing patterns of sexual exploitation,[7] with criminal groups dedicated to sexual exploitation quick to adapt their ways of working, by escalating the use of online communication.[8]

These findings reflect trends reported by Australian authorities. Over a period of 12 months across 2019-20, the AFP's Australian Centre to Counter Child Exploitation (ACCCE) intercepted more than 250,000 CAM files online and 134 children – 67 in Australia – were removed from harm in the 2019-20 financial year.[9] In 2020, the ACCCE Child Protection Triage Unit received more than 21,000 reports of online child sexual exploitation. Each

[5] International Covenant on Civil and Political Rights - Human rights at your fingertips - Human rights at your fingertips | Australian Human Rights Commission
[6] A/HRC/46/31 - E - A/HRC/46/31 -Desktop (undocs.org), P5
[7] Ibid 6, P7
[8] Ibid 6, P11
[9] Nationwide Operation Molto removes 16 children from harm | Australian Federal Police (afp.gov.au)

report contained images and videos of children being sexually assaulted or exploited for the sexual gratification of online child sex offenders. The AFP charged a total of 235 people with 2772 alleged child abuse-related offences in 2020-21.

During the COVID-19 pandemic the ACCCE identified new users of dark web child exploitation sites seeking advice and guidance regarding avoiding detection by law enforcement. Concurrently, the sharing of CAM uploads with the tag 'original content' increased substantially.[10] In addition, the volume of livestreamed abuse increased, with AUSTRAC reporting a "three-fold" increase of suspicious financial transactions indicating payment for such content in 2019-20.[11]

The increasing proliferation of CAM live streaming is particularly concerning given the 'real time' and interactive nature of the offending involved. As noted by the Australian Institute of Criminology (AIC), offenders often request how they want the child victim to be sexually abused either before or during the live streaming session.[12] While not geographically confined, the Philippines has been identified by global law enforcement agencies as a major 'hub' for CAM live streaming, a perfect storm of poverty, readily available children and fast internet.[13] It has been reported the cost of a live stream is as little as AU$14–$57,[14] and Australian men have been identified as some of the most voracious consumers. [15] For victims, their live streamed sexual abuse presents a unique form of trauma, resulting from the continued availability of CAM in which they appear.[16] This form of CAM also presents a significant challenge to law enforcement due to the extra-territorial nature of the offending and difficulty in locating and rescuing victims.

A desktop review undertaken by the CSCRC using records from the Australasian Legal Information Institute found from the beginning of 2021 through to 31 July, 47 sentences had been handed down in higher courts for CAM-related offences. This does not take into account matters heard in lower courts. Reading such judgements, the significant scale and reach of online CAM becomes apparent. For example, in one case, where an offender had downloaded about 3000 CAM files, police reported the likely number of unique victims to

---

[10] Parliamentary Joint Committee on Law Enforcement, *Inquiry into criminal activity and law enforcement during the COVID-19 pandemic*, AFP submission, P4
[11] AUSTRAC Annual Report 2019-20, P178
[12] Australians who view live streaming of child sexual abuse: An analysis of financial transactions (aic.gov.au), P2
[13] Ibid 13, P2
[14] Ibid 13, P3
[15] Regional-Overview_Southeast-Asia.pdf (ecpat.org), P44
[16] Criminal justice responses to child sexual abuse material offending: A systematic review and evidence and gap map (aic.gov.au), P2

be about 600 children.[17] It is interesting to note that in multiple cases, offenders were detected by investigators posing as children on social media platforms, highlighting the difficulties police face in identifying online offenders in the 'real world'. All offenders were male and ranged from being unemployed to IT professionals and geologists.

The efficacy of and any gaps in the legislative tools and tactics of law enforcement used to investigate and prosecute offenders;
and
Opportunities and suitability of streamlining legislative constraints to enable faster investigations that can better respond to rapidly evolving trends in offending.

Law makers are well aware of the online proliferation of CAM, with the Commonwealth Department of Public Prosecutions (CDPP) noting the increasing sophistication of offending facilitated by the internet and encryption.[18] The CDPP states: *"Cases can involve hundreds of thousands of depraved and disturbing images of children and the scale and seriousness of this industry poses challenges for investigation and prosecution. Dealing with such material requires investigators, prosecutors and courts to deal with chat logs, images, videos and written material of a disturbing nature involving exploitation and harm to children"*.[19]

Given the scale of some investigations, the investigative challenges presented by the use of encrypted and dark web communications, and the potential trauma these investigations can have on investigators, there is an increasing need for the law to keep pace with technology. While there is no doubt law enforcement do an excellent job of investigating such crimes, as illustrated by the case studies in this submission, investigation is often slow and, in a digital world, reliant on laws that are no longer fit for purpose. The key pieces of Commonwealth legislation that deals with online CAM is the *Criminal Code*, namely 'carriage service' offences.[20] While these offences provide an effective framework via which an offender can be *charged*, they are not helpful in terms of *investigation*. Greater powers to access encrypted communications and dark web communities are required to assistant law enforcement tackle the scourge of CAM.

[17] R v Appleby [2021] ACTSC 55 (9 April 2021)
[18] Child Exploitation | Commonwealth Director of Public Prosecutions (cdpp.gov.au)
[19] Ibid 19
[20] Ibid 19

Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020

One such legislative mechanism, which is currently before the parliament, is the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* (the Bill). If passed, it will play a key role in countering serious cyber-enabled crime committed domestically and offshore. In particular, the introduction of account takeover warrants will mean authorities will no longer be required to ask serious criminals, including child sex offenders. for permission to access online accounts, as is currently the case.

While the powers authorised under the Bill are undoubtedly extraordinary, the CSCRC submits they are proportionate and appropriate in relation to the threat posed. Furthermore, to ensure such extraordinary powers are not misused, exploited or subject to 'legislative creep', the Bill contains a number of key safeguards and protections. It presents a clear opportunity for Australia to ensure domestic laws are properly aligned with digitally perpetrated activities, allowing lawful access to data and devices where it is appropriate to do so. The Bill seeks to amend the *Surveillance Devices Act 2004*[21] (SD Act), the *Crimes Act 1914*[22] (Crimes Act) and other associated legislation to introduce new powers for the Australian Federal Police (AFP) and the Australian Criminal Intelligence Commission (ACIC) to enhance the investigation and disruption of online crime.

The Bill introduces three new warrants:

- data disruption warrants;
- network activity warrants;
- account takeover warrants.

Data disruption warrants would permit the disruption of data through modification and deletion to frustrate the commission of serious offences.[23] Network activity warrants would prohibit the collection of intelligence on serious criminal activity carried out by criminal networks operating online.[24] Account takeover warrants would allow authorities to take control of a person's online account/s to gather evidence and to further a criminal investigation.[25]

Amendments to the Telecommunications (Interception and Access) Act 1979

One of the greatest challenges Australia's law enforcement and intelligence agencies have faced is accessing data to bring cyber criminals to justice, because much of this data is

[21] Surveillance Devices Act 2004 (legislation.gov.au)
[22] Crimes Act 1914 (legislation.gov.au)
[23] Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 (homeaffairs.gov.au)
[24] Ibid 24
[25] Ibid 24

stored offshore. Recently passed amendments to the *Telecommunications (Interception and Access) Act 1979* via the *Telecommunications Legislation Amendment (International Production Orders) Bill*, however, have enlivened provisions of the United States' *Clarifying Lawful Overseas Use of Data Act* (the CLOUD Act). The CLOUD Act enables access by foreign partners to electronic information held by US-based global providers, information critical to investigations of serious crime. As noted by former Minister for Home Affairs, Peter Dutton: *"the Act creates a new paradigm: an efficient, privacy and civil liberties-protective approach to ensure effective access to electronic data through executive agreements between the United States and trusted foreign partners"*.

Through the amendments, three types of international production orders are now permitted: for interception of data; access to stored communications; and access to telecommunications data. These can be sought for the investigation of a serious offence, monitoring individuals subject to control orders, and for the Australian Security Intelligence Organisation to carry out its national security functions more efficiently.

As a result of the amendments, authorities will no longer have to rely on the cumbersome and outdated mutual legal assistance regime, with data requests that previously may have taken years to process now accelerated to a processing time of just months. The amendments also represent a breakthrough in CAM investigations, enabling Australian authorities to gain access more quickly to offshore data needed in the course of investigations. For example, such data could be sought from a US-based social media platform, app or telco.

Protecting law enforcement from trauma

There is no doubt undertaking CAM investigations can be traumatic for the law enforcement officers involved, especially those who must view CAM as part of the investigative process. Research indicates these officers are at increased risk of experiencing psychological distress and burnout.[26] Given the need to protect law enforcement from as much trauma as possible, there is a key role for technology to play – especially artificial intelligence (AI) and machine learning (ML) – in helping shield investigators from CAM material.

Automated detection of CAM via AI and ML technologies, which are currently being deployed by law enforcement agencies, mean investigators view far less traumatic content, as the materials are identified and classified automatically. Research continues to improve

[26] Patrick Brady, *Crimes Against Caring: Exploring the risk of secondary traumatic stress, burnout and compassion satisfaction among child exploitation investigators*, Journal of police and criminal psychology, 12/2017, Volume 32, Issue 4, P305

these capabilities and in 2019 the Australian Federal Police (AFP) and Monash University launched the AI for Law Enforcement and Community Safety Lab. The Lab is focussed on researching explainable algorithms, ML classification algorithms for illicit image video and text, frameworks for ethical AI as well as techniques for leveraging massive law enforcement datasets.[27]

Case study: Shannon McCoole

In 2015, former Families South Australia carer Shannon Grant McCoole was sentenced to 35 years' jail for his role as leader of a worldwide dark web child pornography ring, which had more than 45,000 members, and for abusing at least seven children in his care.

The website required members to post new child exploitation material every 30 days in order to retain membership, utilising TOR computer software to mask their identity.

Membership came with designated access to different areas of the forum, access to the rules of membership and technical forums directed towards encryption, software and internet safety advice. Members also had access on private areas where there was discussion surrounding the sexual abuse of children and 'rare content'. In addition, members could become special VIPs, honorary members or Private Zone members.

In 2014, authorities became aware the head administrator of the site was an Australian, most likely located in Adelaide. After painstaking police work, McCoole was located after an investigator matched his online vernacular and a freckle on his hand (as seen in dark web CAM content he had posted) to public posts he had made.

McCoole signed over his online identities to police. However, if he had not agreed to this, police would have been unable to lawfully access his accounts. Ultimately, the take-over of McCoole's accounts led to multiple arrests in Australia and overseas and the dismantling of the site. Such a case highlights how network activity warrants and account takeover warrants as proposed under the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* could be used in a highly targeted way to detect and apprehend such offenders more quickly and efficiently.[28]

[27] AiLECS Lab - Faculty of Information Technology | Monash University
[28] Record sentence for head administrator of paedophile site | Commonwealth Director of Public Prosecutions (cdpp.gov.au)

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

Encrypted messaging apps

Encryption is the conversion of information or data into unintelligible code, which prevents unauthorised access. While it provides a key role in keeping personal and valuable information protected, it is also widely used by criminals to cloak their illicit activities.

Encryption makes it difficult for law enforcement to intercept and read messages criminals send each other and to trace cryptocurrency increasingly used to fund criminal enterprise. End-to-end encryption provides a form of communication protection that prevents third parties – including internet service providers, app hosts and law enforcement – from accessing data transferred from one system or device to another. This means data is encrypted on one system or device and only the recipient can decrypt it.

Encrypted instant messaging apps use end-to-end encryption to ensure only the person you send messages to is able to read them. Encryption software built into these apps means a third-party intercepting the messages cannot read them, as they will be indecipherable. These services operate 'over the top' of traditional telephony networks, which means it is impossible to know when they are even being used. Examples of well-known encrypted instant messaging apps include Telegram and WhatsApp.

Facebook Messenger is not currently encrypted by default, but this feature can be enabled. There is a high risk that if, as planned, Facebook adopts end-to-end encryption across its services, it will act as a new forum through which child sex offenders can conceal their communications and activities. Such concerns have been raised by Department of Home Affairs Secretary, Mike Pezzullo, who told a Senate Estimates hearing in 2020 that: "We are particularly concerned about Facebook's plans to go to end-to-end encryption of their entire platform to create, in effect, the world's biggest dark web".[29] It has also been reported that 40-60 per cent of referrals to the Australian Federal Police for child exploitation involve Facebook.[30]

[29] Hansard - Committee 19/10/2020 Parliament of Australia (aph.gov.au)
[30] Facebook accounts for up to 60pc of child abuse reports to AFP, data shows (smh.com.au)

Telegram and WhatsApp remain the "platforms of choice" for many criminals, including child sex offenders.[31] In addition to end-to-end encryption, Telegram offers a suite of features that make it attractive to criminals, allowing multiple levels of communications, from private to public, via one platform, and even features a self-destruct timer that allows messages to permanently disappear after a stipulated period.[32] While some of Telegram's policies have changed and its operators have begun to collaborate (to an extent) with law enforcement,[33] it is unlikely criminals will migrate from the platform in the foreseeable future given its features, familiarity and ease of use. Some other encrypted messaging apps used by criminals include Surespot, Signal, Wickr, Kik, ChatSecure, BCM, Gab Chat, Hoop Messenger, Riot.im, Rocket.Chat and TamTam.[34]

The dark web

The dark web is not like the surface web, the external interface of the internet most people are familiar with. It is part of the internet that evades indexing by search engines, instead requiring the use of an anonymising browser (like Tor) that routes traffic through multiple servers, encrypting it along the way. To help ensure anonymity, dark web browsers isolate sites to prevent tracing, automatically clear browsing history, prevent surveillance of connections, clone or dupe users' appearances to avoid fingerprinting and relay and encrypt traffic three times as it runs across the network. Because access to specific secret sites is required, criminals that use the dark web to plan their activities can hide these activities and work hard to ensure that their groups are not infiltrated by law enforcement. Hence, given the anonymity the dark web affords, it is unsurprising it has been exploited by a wide range of criminal actors, including those producing and seeking CAM.

Case study: CDPP v CCQ (Pseudonym)

In 2019, CCQ, aged 41, had his sentence increased to 16 years' jail on appeal for the transmission and possession of thousands of files containing the most extreme and disturbing level of CAM content.[35] Between 1 January 2016 and 18 November 2017 CCQ used a number of messaging and social media applications including Telegram and Kik to

[31] GNET-Report-Migration-Moments-Extremist-Adoption-of-Text-Based-Instant-Messaging-Applications_V2.pdf (gnet-research.org), P1
[32] 181221_EvolvingTerroristThreat.pdf (csis-website-prod.s3.amazonaws.com), P33
[33] Ibid 33, P5
[34] Ibid 32, P1
[35] Commonwealth Director of Public Prosecutions v CCQ [2021] QCA 4 (22 January 2021) (austlii.edu.au)

transmit, solicit, access and receive child abuse material, and in that period he possessed a quantity of child abuse material on electronic devices or online accounts.

The offences were committed for sexual gratification. CCQ's self-professed sexual interest was in the abuse, exploitation and degradation of very young children, particularly babies and toddlers. The material showed very young children, including newborn babies and toddlers, subjected to acts of rape, incest, bestiality and extreme cruelty. The nature of his proclivities was indicated by his responses to various online persons, as being interested in "0 to five" and "I love baby and brutal".

In November 2017 police executed a search warrant at CCQ's home. Initially he told police he had nothing to declare. While providing passwords for his online accounts in compliance with a court order, when questioned by police, he denied ever using the application Kik or having ever exchanged images of children using social media accounts. Even when police found child abuse material on SD cards at his residence, CCQ initially continued to deny any knowledge, telling police "I've told you as much as I know". Ultimately, however, CCQ made admissions to accessing and possessing CAM.

Between 1 January 2016 and 18 November 2017 CCQ accessed a substantial amount of CAM over the internet, including as many as 5,646 CAM files from Telegram.

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

There is a clear role for technology providers to help law enforcement combat CAM through the detection, removal and reporting of such content and, to an extent, such support is rendered. However, more can be done.

The work of the Technology Coalition, which includes big tech members like Google, Facebook and Microsoft, is a step in the right direction and last year the organisation launched a five-fold plan to combat child sexual abuse on the internet.[36] The aim of the coalition is to support tech companies of all sizes to tackle risks to online child safety through coordinated efforts to improve the detection and reporting of CAM and related materials. [37] It is also important to note the over the past decade, there has been significant progress in the development and roll-out of innovative technology to combat online CAM.

[36] Google, Facebook and Microsoft back plan to combat child sexual abuse (cnbc.com)
[37] The Technology Coalition Announces Project Protect – Technology Coalition

For example, Microsoft's PhotoDNA is used globally to detect, disrupt, and report millions of child sexual exploitation images.[38] Likewise, Google's Content Safety API has improved the ability of NGOs and other tech companies to review CAM and Facebook's open-source photo- and video-matching technology employs hash-sharing systems to communicate, assisting in the detection of duplicated CAM.[39] In the US, Apple recently launched *neuralMatch*, which scans images from Apple devices before they are uploaded to iCloud, and also has plans to scan users' encrypted messages for CAM.[40]

However, as mentioned previously, much of this good work will suffer if Facebook adopts end-to-end encryption, which could stifle the detection and reporting of CAM on its platform. Such reporting is vital given the significant amount of CAM detected on Facebook. For example, in 2020 the US National Centre for Missing and Exploited Children (NCMEC) reported Facebook was responsible for 94 per cent of the 69 million child sex abuse images reported by US technology companies.[41]

How could tech companies be compelled to provide more assistance?

There is scope for a legislative regime to be introduced so that civil or criminal action could be taken against technology providers found to have had CAM published or shared on their platform. Such a regime could introduce significant fines for platforms found in breach, in the same vein as the *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019* (the Act).

In 2019, the Act was swiftly enacted by the Federal Government in the wake of the Christchurch terror attack. It was a pioneering and pivotal move aimed at reducing the use of online platforms to transmit acts of violence.[42] Violent abhorrent material is defined as that which captures a terrorist act involving serious harm or death, murders or attempts to murder, torture, rape and violent kidnapping.[43] The Act created two new criminal offences aimed at internet service providers and hosting and content providers – failure to report and failure to remove violent abhorrent material – holding them responsible for reporting and removing such material.[44] Large financial penalties and imprisonment apply in the case of conviction. The fact no charges have been laid under the Act may serve to demonstrate its deterrent effect.

[38] Ibid 38
[39] Ibid 38
[40] Apple to scan U.S. i

The CSCRC notes content containing rape is currently captured in the Act. This could encapsulate some, but not all, CAM, as the legislation explicitly states genital penetration must occur.[45] There must also be elements of 'violence' for its provisions to be enlivened. Hence, the Act could be amended to capture CAM that meets a particular threshold or, alternatively, consideration could be given to the introduction of a new, similar regime that deals specifically with CAM published or distributed on tech platforms.

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

While some links between the use of online CAM and contact offending have been established, there is no significant evidence to indicate accessing online CAM leads to contact offending or vice versa.

Research has shown CAM offenders differ in demographic and psychological characteristics to those convicted or charged with contact child sexual offences and mixed offences (both contact and CAM offences).[46] CAM offenders are generally younger, of Anglo-Saxon descent, better educated and more likely to have professional employment in contrast to contact and mixed offenders.[47] Interestingly, CAM offenders have been found to "have higher scores on sexual deviance and victim empathy, less emotional identification with children and fewer cognitive distortions than contact offenders".[48] AIC research has noted a "significant relationship" exists between involvement in a CAM network and contact offending,[49] but also notes that a history of online CAM consumption is not indicative of recidivism, nor does it predict contact offending.[50]

When it comes to CAM offending, offenders have a tendency to minimise their behaviour, with the online environment playing a key role in not only breaking down barriers in accessing CAM, but also offering a sense of anonymity and security.[51] ACCCE research indicates that 83 per cent of relevant studies show offenders often perceived their

[45] Ibid 45
[46] Larissa S. Christensen and George S. Tsagaris, Offenders convicted of child sexual exploitation material offences: characteristics of offenders and an exploration of judicial censure, Psychiatry, Psychology and Law, 2020 Vol. 27, No. 4, 647–664
[47] Ibid 47
[48] Ibid 47
[49] Trajectories in online child exploitation offending in Australia (aic.gov.au), P10
[50] Ibid 50, P11
[51] Ibid 2

offending behaviour as harmless. It also shows the type of material viewed often escalates from the viewing of normative adult pornography to CAM and more extreme material.[52]

Parental offending

When considering matters pertaining to the production and distribution of CAM, one issue not discussed enough is parental involvement in such offending. While uncomfortable, it is necessary to shine a light on what is an important issue.

Research has found a significant proportion of CAM is produced and distributed by parents who victimise their children.[53] The AIC has identified parental production as a major challenge to the prevention and detection of CAM.[54] This is because, within the home environment, access to vulnerable children and opportunities for offending can lead to serious abuse, with little chance of offenders being detected.[55] The AIC has highlighted the need for targeted research into CAM production perpetrated by parental figures to help develop strategies to prevent and detect such offending.[56]

Case study: R v G [2021] NSWDC

On 26 February 2021, G was sentenced to 15 years' jail for contact offending against three of his step granddaughters (aged one, three and eight at the time of offending) and the historical sexual abuse of his stepdaughter, as well as the production and possession of CAM, transmitted on the dark web. This case is relevant because the offender committed both contact and online offences.

In early 2019, while conducting investigations on a number of dark web sites known to facilitate the sharing of CAM, investigators from Task Force Argos (Qld Police) commenced monitoring a user called *GrandDadof6*, with alternative usernames including *AusPedo*. It was evident the user was responsible for sharing newly produced material featuring the sexual abuse of more than one female child and that he was responsible for production of the material. Investigators deduced the user was located in NSW and in April 2019, member of the NSW Police Force Child Exploitation Internet Unit began an investigation into the images to identify the victims and offender. A school principal was able to identify one of the children in the images, who was a student at his school and was aged nine.

[52] Ibid 2
[53] Production and distribution of child sexual abuse material by parental figures (aic.gov.au), P2
[54] Ibid 54, P2
[55] Ibid 54, P2
[56] Ibid 54, P2

Police then identified the girl's step-grandfather as a suspect, who was subsequently arrested and charged, pleading guilty.

When questioned, the offender told police that "in between doing all that (contact offending), I just sort of started taking pictures". He uploaded those photos to his hard drive and shared them online. He told police he used the dark web multiple times a week and, in relation to the large amount of additional child abuse material found on his computer and storage devices, the offender stated he downloaded it for enjoyment.