Inquiry into Law Enforcement Capabilities in Relation to Child Exploitation

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

Contents

Introduction

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

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

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

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

Background

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

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

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

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

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

Are CSAM offenders different to contact sexual offenders?

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

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

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

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

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

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

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

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

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

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

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

What proportion of CSAM offenders commit contact sexual offences?

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

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

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

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

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

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

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

CSAM is a complex and constantly evolving crime

How much CSAM offending is detected?

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

CSAM offenders encourage each other online to sexually abuse children

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

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

Online grooming can lead to contact sexual abuse

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

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

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

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

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

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

Live streaming of child sexual abuse

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

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

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

Use of encryption by offenders

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

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

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

Meta plans to implement universal end-to-end encryption on Facebook Messenger and Instagram's private messages in 2023 (Davis 2021; Kent 2021). These are two of the largest social media platforms in the world. There are concerns that CSAM detection technologies currently used by these platforms (eg PhotoDNA, artificial intelligence tools) will not work in an end-to-end encryption

environment as they will be unable to decrypt the content and scan it for CSAM (NCMEC 2019). To our knowledge, Meta has not publicly proposed a strategy to maintain its ability to detect and report CSAM on these platforms once it introduces end-to-end encryption next year. As most CSAM on Facebook Messenger is detected using PhotoDNA and artificial intelligence tools (Facebook nd; Farid 2019), NCMEC has estimated that Meta's implementation of end-to-end encryption across all its major platforms will reduce the number of CSAM reports it receives by more than 50 percent (NCMEC 2019). This does not mean that CSAM offending will be reduced; rather, Meta will no longer be able to detect it.

Role of tech companies

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

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

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

Implications for ESPs

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

Secondly, more responsibility should be placed on ESPs to prevent CSAM from being uploaded in the first instance. These platforms should adopt evidence-based methods such as pop-up warning messages, which can deter the viewing or sharing of CSAM and refer individuals to sources of help (Prichard et al. 2022). Deterrence messaging campaigns can also reach large numbers of individuals (Grant et al. 2019). These tools should also be evaluated; Meta currently uses pop-up warning

messages to deter child sexual exploitation, yet there is no information publicly available on their impact or effectiveness.

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

Implications for international law reform

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

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

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

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

Summary

Link between online and contact sexual offending

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

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

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

Encryption used by online offenders

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

The role of tech companies in protecting children from harm

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

References

URLs correct as at October 2022

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

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

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

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

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

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

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

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

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

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

Bursztein E, Clarke E, DeLaune M, Elifff DM, Hsu N, Olson L, Shehan J, Thakur M, Thomas K & Bright T 2019. Rethinking the detection of child sexual abuse imagery on the internet. International World Wide Web Conference, San Francisco, 13–17 May: 2601–2607. https://doi.org/10.1145/3308558.3313482

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

Dowling C, Boxall H, Pooley K, Long C & Franks C 2021. Patterns and predictors of reoffending among child sexual offenders: A rapid evidence assessment. *Trends & issues in crime and criminal justice* no. 632. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti78306

ECPAT International 2017. *Online child sexual exploitation: An analysis of emerging and selected issues.* ECPAT International Journal 12: 1–63. https://humantraffickingsearch.org/resource/online-child-sexual-exploitation-analysis-emerging-selected-issues/

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

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

eSafety Commission 2020. End-to-end encryption trends and challenges: Position statement. Sydney: eSafety Commissioner. https://www.esafety.gov.au/about-us/tech-trends-and-challenges/end-end-encryption

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

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

Europol 2017. *Online sexual coercion and extortion as a form of crime affecting children: Law enforcement perspective*. The Hague: Europol. https://www.europol.europa.eu/publications-events/publications/online-sexual-coercion-and-extortion-form-of-crime-affecting-children-law-enforcement-perspective

Facebook nd. Community standards enforcement report: Child endangerment: Nudity and physical abuse and sexual exploitation. https://transparency.fb.com/data/community-standards-enforcement/child-nudity-and-sexual-exploitation/facebook/

Farid H 2019. *Testimony: House Committee on Energy and Commerce: Fostering a healthier internet to protect consumers*. Washington DC: House Committee on Energy and Commerce. https://energycommerce.house.gov/committee-activity/hearings/hearing-on-fostering-a-healthier-internet-to-protect-consumers

Gewirtz-Meydan A, Walsh W, Wolak J & Finkelhor D 2018. The complex experience of child pornography survivors. *Child Abuse & Neglect* 80: 238–248. https://doi.org/10.1016/j.chiabu.2018.03.031

Grant B, Shields B, Tabachnick J & Coleman J 2019. "I didn't know where to go": An examination of Stop It Now!'s sexual abuse prevention helpline. *Journal of Interpersonal Violence* 34(20): 4225–4253. https://doi.org/10.1177/0886260519869237

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

Hailes H, Yu R, Danese A & Fazel S 2019. Long-term outcomes of childhood sexual abuse: An umbrella review. *The Lancet: Psychiatry* 6(10): 830–839. https://doi.org/10.1016/S2215-0366(19)30286-X

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

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

Insoll T, Ovaska AK, Nurmi J, Aaltonen M & Vaaranen-Valkonen N 2022. Risk factors for child sexual abuse material users contacting children online: Results of an anonymous multilingual survey on the dark web. *Journal of Online Trust & Safety* 1(2). https://doi.org/10.54501/jots.v1i2.29

International Justice Mission (IJM) 2020. *Online sexual exploitation of children in the Philippines: Analysis and recommendations for governments, industry and civil society: Summary report*. IJM. https://www.ijm.org/vawc/blog/osec-study

Internet Watch Foundation (IWF) 2018. *Trends in child sexual exploitation: Examining the distribution of captures of live-streamed child sexual abuse.* Cambridge, UK: Internet Watch Foundation. https://www.iwf.org.uk/about-us/why-we-exist/our-research/

Interpol 2020. *Threats and trends: Child sexual exploitation and abuse: COVID-19 impact.* Lyon: Interpol. https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-highlights-impact-of-COVID-19-onchild-sexual-abuse

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

Kent G 2021. Messenger policy workshop: Future of private messaging. https://about.fb.com/news/2021/04/messenger-policy-workshop-future-of-private-messaging/

Krone T, Smith RG, Cartwright J, Hutchings A, Tomison A & Napier S 2017. *Online child sexual exploitation offenders: A study of Australian law enforcement data.* Report to the Criminology Research Advisory Council. CRG 58/12–13. Canberra: Australian Institute of Criminology. https://www.aic.gov.au/crg/reports/crg-5812-13

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

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

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

Morgan A 2022. *Exploring the role of opportunity in recidivist child sexual offending.* Research Report no. 24. Canberra: Australia Institute of Criminology. https://doi.org/10.52922/rr78719

Murdoch L 2016. Australian accused of child sex tourism arrested in the Philippines. *Sydney Morning Herald*, 1 September. https://www.smh.com.au/world/australian-accused-of-child-sex-tourism-arrested-in-thephilippines-20160901-gr6x8x.html

Napier S, Teunissen C & Boxall H 2021. Live streaming of child sexual abuse: An analysis of offender chat logs. *Trends & issues in crime and criminal justice* no. 639. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti78375

National Centre for Missing and Exploited Children (NCMEC) 2022a. CyberTipline 2021 report. https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata

National Center for Missing and Exploited Children 2022b. Sextortion. National Center for Missing and Exploited Children. https://www.missingkids.org/theissues/sextortion

National Center for Missing and Exploited Children (NCMEC) 2021. 2020 CyberTipline reports by electronic service providers (ESP). https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata#reports

National Center for Missing and Exploited Children (NCMEC) 2019. NCMEC's statement regarding end-to-end encryption. https://www.missingkids.org/blog/2019/post-update/end-to-end-encryption

Netclean 2020. *Netclean report: COVID-19 impact 2020: A report about child sexual abuse crime.* https://www.netclean.com/knowledge

Netclean 2019. *Netclean report 2019: A report about child sexual abuse crime.* https://www.netclean.com/knowledge

Ogloff J, Cutajar M, Mann E & Mullen P 2012. Child sexual abuse and subsequent offending and victimisation: A 45 year follow-up study. *Trends & issues in crime and criminal justice* no. 440. Canberra: Australian Institute of Criminology. https://www.aic.gov.au/publications/tandi/tandi440

Patchin J & Hinduja 2020. Sextortion among adolescents: Results from a national survey of U.S. youth. *Sexual Abuse* 32(1): 30–54. https://doi.org/10.1177/1079063218800469

Prichard J & Spiranovic C 2014. *Child exploitation material in the context of institutional child sexual abuse*. Report for the Royal Commission into Institutional Responses to Child Sexual Abuse. https://www.childabuseroyalcommission.gov.au/research

Prichard J, Wortley R, Watters P, Spiranovic C, Hunn C & Krone T 2022. Effects of automated messages on internet users attempting to access "barely legal" pornography. *Sexual Abuse* 34(1): 106–124. https://doi.org/10.1177/10790632211013809

Salter M & Hanson E 2021. "I need you all to understand how pervasive this issue is": User efforts to regulate child sexual offending on social media. In J Baily, A Flynn & N Henry (eds), *The Emerald international handbook of technology facilitated violence and abuse*. Emerald Publishing: 729–748. https://doi.org/10.1108/978-1-83982-848-520211053

Schiemer J 2018. Strong and responsible: Can encryption be both? *FlagPost*, 3 October. https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/FlagPost/2018/October/Encryption

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

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

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

Statista 2022a. Most popular global mobile messenger apps as of January 2022, based on number of monthly active users (in millions). https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/

Statista 2022b. Number of Instagram users worldwide from 2020 to 2025 (in millions). https://www.statista.com/statistics/183585/instagram-number-of-global-users/

Stevens D 2020. Consumers seek out apps with enhanced privacy features to keep in touch in our new normal. https://www.data.ai/en/insights/market-data/consumers-seek-enhanced-privacy-app-features/

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

Teunissen C, Boxall H, Napier S & Brown R 2022. The sexual exploitation of Australian children on dating apps and websites. *Trends & issues in crime and criminal justice* no. 658. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti78757

Teunissen C & Napier S 2022. Child sexual abuse material and end-to-end encryption on social media platforms: An overview. *Trends & issues in crime and criminal justice* no. 653. Canberra: Australian Institute of Criminology. http://doi.org/10.52922/ti78634

Teunissen C & Napier S forthcoming. The co-occurrence of child sexual abuse live streaming and other forms of child exploitation. *Trends & issues in crime and criminal justice*. Canberra: Australian Institute of Criminology

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

Torres-Cortez R 2022. 'Sextortion' crimes against children increasing, FBI says. *Las Vegas Review-Journal*, 5 May. https://www.reviewjournal.com/crime/sex-crimes/sextortion-crimes-against-children-increasing-fbi-says-2572147/

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

Wakefield J 2021. Apple delays plan to scan iPhones for child abuse. *BBC News*, 3 September. https://www.bbc.com/news/technology-58433647

WhatsApp 2020. Two billion users – Connecting the world privately. https://blog.whatsapp.com/two-billion-users-connecting-the-world-privately

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

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

Appendix: Recent and forthcoming AIC research on child sexual exploitation

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

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

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

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

Cubitt T, Napier S & Brown R 2021. Predicting prolific live streaming of child sexual abuse. *Trends & issues in crime and criminal justice* no. 634. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti78320

Dowling C, Boxall H, Pooley K, Long C & Franks C 2021. Patterns and predictors of reoffending among child sexual offenders: A rapid evidence assessment. *Trends & issues in crime and criminal justice* no. 632. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti78306

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

Eggins E et al. 2021. Criminal justice responses to child sexual abuse material offending: A systematic review and evidence and gap map. *Trends & issues in crime and criminal justice* no. 623. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti78023

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

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

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

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

Morgan A 2022. *Exploring the role of opportunity in recidivist child sexual offending.* Research Report no. 24. Canberra: Australia Institute of Criminology. https://doi.org/10.52922/rr78719

Napier S, Teunissen C & Boxall H 2021. Live streaming of child sexual abuse: An analysis of offender chat logs. *Trends & issues in crime and criminal justice* no. 639. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti78375

Napier S, Teunissen C & Boxall H 2021. How do child sexual abuse live streaming offenders access victims? *Trends & issues in crime and criminal justice* no. 642. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti78474

Prichard J et al. 2022. Warning messages to prevent illegal sharing of sexual images: Results of a randomised controlled experiment. *Trends & issues in crime and criminal justice* no. 647. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti78559

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

Salter M & Woodlock D forthcoming. Secrecy, control and violence in women's intimate relationships with child sexual abuse material offenders. *Trends & issues in crime and criminal justice*. Canberra: Australian Institute of Criminology

Teunissen C, Boxall H, Napier S & Brown R 2022. The sexual exploitation of Australian children on dating apps and websites. *Trends & issues in crime and criminal justice* no. 658. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti78757

Teunissen C & Napier S 2022. Child sexual abuse material and end-to-end encryption on social media platforms: An overview. *Trends & issues in crime and criminal justice* no. 653. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti78634

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

Westlake B et al. 2022. Developing automated methods to detect and match face and voice biometrics in child sexual abuse videos. *Trends & issues in crime and criminal justice* no. 648. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti78566

Sarah Napier is the Manager of the Online Sexual Exploitation of Children Research Program at the Australian Institute of Criminology.

Dr Rick Brown is the Deputy Director of the Australian Institute of Criminology.