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

Associate Professor Benoit Leclerc
School of Criminology and Criminal Justice, Griffith University
Griffith Criminology Institute, Griffith University[1]

Associate Professor Jesse Cale
School of Criminology and Criminal Justice, Griffith University
Griffith Criminology Institute, Griffith University

Professor Thomas Holt
School of Criminal Justice, Michigan State University, USA

August 2021

[1]Please send correspondence to A/Prof Benoit Leclerc, Griffith University | School of Criminology & Criminal Justice/Griffith Criminology Institute | MT Gravatt Campus | 176 Messines Ridge Road | Brisbane Qld 4122 Australia. Office: +61 7 3735 5755 | Mobile: +61 479 186 522
Email: b.leclerc@griffith.edu.au

Dear Parliamentary Joint Committee on Law Enforcement,

We welcome the opportunity to provide a written submission to the Parliamentary Joint Committee on Law Enforcement's inquiry into law enforcement capabilities in relation to child exploitation. This submission is informed by the authors' recently completed research into *Boosting Crime Prevention and Crime Detection Capabilities of Online Investigators: A Script Analysis of Creation and Distribution of Child Exploitation Material*, a research grant funded by the Australian Institute of Criminology as part of the Child Sexual Abuse Material Reduction Research Program.

In various sections of this submission we draw on our research findings from this project including: a systematic review of crime commission processes in child sexual abuse material production and distribution (Cale, Holt, Leclerc, Singh, & Drew, 2021); a review assessing the challenges affecting the investigative methods to combat online child exploitation material offences (Holt, Cale, Leclerc, & Drew, 2020); a report examining how child sexual abuse material offenders operate on the Dark Web (Leclerc, Drew, Holt, & Cale, 2021a; Leclerc, Drew, Holt & Cale, 2021b), and a study providing evidence on training and support needed to combat child sexual exploitation online (Leclerc, Cale, Holt & Drew, in preparation).

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

- Several reports suggest that online child sexual exploitation is increasing dramatically not only in Australia but worldwide (International Center for Missing & Exploited Children, 2021). For instance, a report from the Internet Watch Foundation (IWF, 2019) confirmed the existence of 132,676 URLs or web pages to contain, link to, or advertise child exploitation material (CEM) across 4,956 domains traced to 58 countries - a 27% increase since 2018. In addition, the report confirmed the identification of 288 new dark web sites selling this material – an increase of 238% since 2018. Another recent major report on CEM production and distribution has identified a trend toward more egregious sexual content over time (Seto et al., 2018).

- There is also growing evidence suggesting that offenders are now using virtual currencies to trade CEM. In fact, the IWF (2019) indicated that most of the identified websites in 2018 were commercial and only accepted payment in virtual currencies (e.g., Bitcoin). According to the IWF (2019), the last several years have seen the greatest overall rise of Dark Web markets engaged in the sale of CEM.

- A recent report from the Egmont Group of Financial Intelligence Units (2020) indicated that the growth in online streaming of child sexual exploitation for financial gain has been facilitated by the expanding reach of 4G, and recently 5G, in many parts of the world including developing countries (see also Brown, Napier and Smith, 2020). Critically, live streaming can also lead to offenders travelling to other countries to sexually exploit children, commonly known as child sex tourism, and even extend to human trafficking (International Centre for Missing and Exploited Children (ICMEC), 2021).

- CEM can be accessed on the Open Web or Dark Web. CEM content on the Open Web is accessible via traditional web browsers and may have been indexed via search engines such as Google. Additionally, the content is hosted on web servers that provide

information about the physical location of the materials and a degree of detail about the site operators (Andress & Winterfeld, 2013). A recent Internet Watch Foundation (2018) report indicated that most webpages hosting CEM were image-hosting websites (82%), followed by cyberlockers (file-hosting sites, 5%), and banner sites (4%). Other types of webpages that were identified as hosting such material included blogs, websites, forums, search providers, image boards, video channels, and social networking sites (IWF, 2018).

- In contrast to the Open Web, accessing CEM on the Dark Web requires the use of specialized encryption software and browser utilities such as Tor (Aldridge et al., 2018). These tools hide the IP address and location details of both users and the servers that host content, making it difficult to track individuals' behaviours. Additionally, the Dark Web content is not indexed through traditional search engines, which complicates the process of identifying websites without some knowledge of their existence (Aldridge et al., 2018; Copeland et al., 2019).

- CEM production occurs in a variety of contexts including, but not limited to: intrafamilial relationships; online grooming and solicitation; and, offline grooming and solicitation (see Wolak et al., 2011). In a study by Wolak et al. (2011) the most common tactics employed by producers of CEM involved coercion and pressure or using romance or a friendship to persuade the victim. Generally speaking, offenders use a range of manipulative strategies to engage victims and achieve their compliance online for sexual purposes (e.g., Kloess, Hamilton-Gilchritsis & Beech, 2019; Kloess, Seymour-Smith, Hamilton-Giachritsis, Long, Shipley and Beech, 2017) in a similar way that offenders manipulate victims offline for contact sexual offending (e.g., Leclerc, Beauregard & Proulx, 2009; Leclerc & Cale, 2015; Leclerc et al., 2011; Leclerc, Smallbone & Wortley, 2013).

- Child sex trafficking is another important context in which CEM production takes place. A study by Reid (2016) showed that sex traffickers not only engaged in the prostitution of minors but also actively created sexually explicit media of them. In some cases, traffickers shared these photos on the internet or used them to blackmail the victims; this is often a key component of the overall crime commission process associated with sex trafficking. In effect, CEM production is often used as a tool to gain control over victims to facilitate other forms of child sexual exploitation (e.g., prostitution).

- CEM offenders operate in specific ways to consume, distribute and/or produce CEM online. A crime commission process containing several steps that offenders go through to gain access to the Dark Web and consume, distribute, and/or produce CEM online has been recently identified (Leclerc et al., 2021a; b). These include: 1) searching the Open Web for CEM content; 2) finding the existence of Dark Web; 3) setting up access to Dark Web; 4) entering the Dark Web; 5) accessing CEM content; 6) protecting their identity; 7) engaging with other members of CEM related groups; and 8) consuming and/or distributing CEM. Several additional steps are involved for offenders producing CEM on the Dark Web and these particular offenders are characterised by a very high level of engagement in CEM/Dark Web.

- After engaging with CEM on the Dark Web for the first time, offenders will generally proceed in one of the following three ways: (1) consume CEM and leave the Dark Web,

(2) consume and distribute CEM on the Dark Web, or (3) increase their involvement in CEM activities on the Dark Web to the extent of producing CEM for instance.

- The first way simply involves individuals who view CEM and then leave the Dark Web. One reason for this pattern may include the difficulty of navigating the Dark Web, another is a lack of interest in interacting with other individuals on the Dark Web.

- The second way involves individuals who will repeat the above process but engage more actively in consuming and distributing CEM on the Dark Web. Many of these individuals engage in repeated consumption and distribution of CEM because they find a platform to express themselves and engage with other individuals who have similar sexual interests (Leclerc et al., 2021).

- The third way involves individuals who will increase their activity on the Dark Web, participating in related online communities of specific groups of individuals with similar interests, and eventually gain an elevated status in these communities (see also Fortin, et al., 2018). These individuals continuously contribute CEM (e.g., by distributing) and often join other related online communities.

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

Challenges facing law enforcement investigations of CEM

- The evolution of technologies and the new and emerging trends in social media platforms are currently and constantly disrupting how CEM investigations can be conducted. For instance, Powell, Cassematis, Benson, Smallbone and Wortley (2014) conducted in-depth qualitative interviews with CEM police investigators in Australia on the challenges involved in their investigations. Participants referred to the importance of having up-to-date computer hardware for backing up large volumes of material and keeping up with offenders. Holt, Cale, Leclerc and Drew (2020) described technological innovations as a central challenge for online investigators. The rise of TOR and the Dark Web provide actors with a degree of anonymity that cannot be mitigated with ease. In addition, some methods to work around encryption and identify offenders may violate legal protections (Broadhurst, 2019). As encrypted communications applications like Signal and Telegram become more popular, the challenges facing investigators increase when dealing with CEM cases (Broadhurst, 2019). Parallel to this is also the rapid increase of adolescents (and even children) owning mobile technology and engaging with social media. All these factors benefit offenders who cannot only find tools to engage with CEM with limited risk of apprehension, but also have ready access to an ever-expanding pool of potential victims. In a study by Leclerc, Cale, Holt and Drew (in preparation), the need to be kept up to date with the new Internet trends and emerging social media platforms (21%) and support regarding knowledge sharing (including knowledge on emerging technological tools and methods to investigate) with other police jurisdictions (14%) emerged as important dimensions for future training and support from the perspective of online investigators.

- Linked to the need for technological resources are workload constraints that investigators are facing (Powell et al., 2014). In the study by Powell et al. (2014), almost all participants felt that the number of CEM investigators was inadequate for meeting the workload at any given time due to circumstances, such as inadequate recruitment of CEM investigators and frequent secondment of investigators temporarily to other policing duties. Participants reported the inappropriateness of certain job requests, coupled with a lack of funding allocated to CEM investigations, as challenging. Participants noted for example that carrying out unrelated policing duties (e.g., security work at a festival) or performing administrative duties delegable to less-specialised staff pulls them away from CEM investigations. This was recently supported by investigators who also reported lacking time to conduct CEM investigations and lacking investigators to ensure an adequate handover of cases and completion of additional administrative tasks. Holt et al. (2020) pointed to the impossible task to manage the sheer quantity of CEM constantly appearing online. Faced with such a high volume of CEM online, online CEM investigators must identify, select, and prioritise the most serious cases among many cases. In addition, there is substantial time and efforts that is spent investigating one case once it has been selected for further investigation, which may further compound the stressors investigators face.

- The efforts of law enforcement agencies can be enhanced by nongovernmental non-law enforcement organizations specializing in the investigation of CEM (Wall, 2007). These agencies have no formal accountability in the broader structure of public corporations and traditional law enforcement agencies. As a result, their operations tend to focus on public functions, including serving as a clearinghouse for information on victimization or attempts to regulate and operate tip-lines for offenses (Wall, 2007).

    - Example: In the United States, the National Center for Missing and Exploited Children (NCMEC) operates as a partially government-funded entity that is congressionally mandated to facilitate the investigation of crimes against children (National Center for Missing and Exploited Children, 2017). They offer myriad services to law enforcement, most notably including a tip line for individuals to report suspected incidents of child abuse, and various forms of CEM (National Center for Missing and Exploited Children, 2017). Additionally, NCMEC operates the Child Victim Identification Program (CVIP), which culls through CEM to determine the identity and location of child victims (National Center for Missing and Exploited Children, 2017). There are numerous similar entities serving domestic and international law enforcement agencies across the globe (Broadhurst, 2019). For instance, the International Center for Missing and Exploited Children (ICMEC) is a non-profit that operates internationally, fulfilling much of the same role as the NCMEC but on a global level (International Center for Missing and Exploited Children, 2017). Additionally, the Internet Watch Foundation (IWF) is a charitable organization located in the United Kingdom that is dedicated to removing CEM and obscene content from the Internet (Internet Watch Foundation, 2017). They operate a tip-line to report CEM and engage in coordinated information sharing with law enforcement and ISPs to facilitate blocking harmful content and investigating CEM.

- An organisation such as the ICMEC, which is already collaborating with different partners, police organisations and the financial sector, can assist with transferring and sharing data collaboratively on CEM knowledge, new trends, and case studies. This high level of collaboration across different sectors (e.g., government, non-government, financial) and organisations is critical to disrupt CEM activities.

Challenges surrounding undercover and covert methods of investigation

- Multinational CEM investigations have proven successful in disrupting CEM networks that produce and distribute CEM. While it may seem complicated to have such networks in place, it is vital given the international distribution systems in place to facilitate CEM distribution. Additionally, the variations in law enforcement investigative tools, knowledge and powers available make it possible for investigators in one nation to share information with investigators in another nation they may not otherwise be able to acquire (Broadhurst, 2019). However, collaboration and requests from police organisations internationally can present other challenges such as putting more time pressure on competent police organisations, such as in Australia.

- Police organisations are facing challenges in how they can conduct their investigations online particularly due to legislative constraints. Recent evidence suggests some CEM groups have moved to Dark Web hosting services in an attempt to shield their location and conceal their participants' activities from law enforcement (Broadhurst, 2019; Hoydal et al., 2017). There have been numerous CEM cases that have faced stark legal challenges due to the rise of Tor and the inherent difficulties present in identifying the location of offenders. For example, in one notable case, due to the protocols that encrypt Tor user communications, agents were unable to observe the actual IP addresses of those visiting the site to affect search warrants or further criminal investigations. As a result, the FBI utilized a “network investigation technique,” or NIT, that consisted of malware that would compromise users' browsers so as to acquire their originating IP address and other information (Garcha, 2018; Weaver, 2016; Widenhouse, 2017). This malware successfully hacked the users' computers and led to a series of arrests against participants and administrators within the site. However, some lawyers for the accused in this case questioned the legality of the NIT employed on the basis of 4th amendment protections in the US (Garcha, 2018; Widenhouse, 2017). Individuals are protected from warrantless search and seizure of evidence in the US, which the use of this malware may have violated because they deliberately compromised users' privacy without appropriate due process (Garcha, 2018; Widenhouse, 2017). Attorneys for individuals arrested in this operation have challenged the legality of the evidence collected against their clients and demanded that the FBI provide more information on the NIT employed to understand how their personal information was acquired (Broadhurst, 2019). In fact, the charges against one individual were dropped because the FBI refused to provide more details on the NIT (Widenhouse, 2017). The attorneys in the case even created a national working group regarding the legality and use of NIT to encourage greater protection of due process rights in the US (Cox, 2016).

- Taken together, the use of undercover law enforcement methodologies may have to evolve carefully so as to minimize failed prosecutions due to the use of anonymization tools by CEM offenders (Broadhurst, 2019). In addition, there is a constant need for

online investigators to learn and be kept up to date with the legislation and procedural requirements related to the conduct of CEM investigations.

- The steps offenders take to set up their access to the Dark Web and CEM give us critical information on how they use information technology skills both to engage with other offenders and consume, distribute and/or produce CEM online. These steps can be used by police organisations and other agencies as potential intervention points to think of measures to disrupt CEM activities (e.g., Leclerc, 2017; Leclerc et al., 2011). Similarly, the data circulated and shared on the Dark Web between offenders on how they produce CEM could be collected in a systematic fashion to enhance the understanding of the entire crime commission process and then re-used for training purposes. In fact, many of the script steps represent promising data points that can be leveraged by the police (see also Lee & Holt 2020).

- Various studies noted that investigators working cybercrime cases feel they do not possess the necessary skills, training, or equipment to affect these crimes (Harkin et al., 2018; Holt et al., 2015; Lee et al., 2019; Stambaugh et al., 2001). Consistent with this, more than half of investigators (55%) recently indicated that social media training as well as training on different types of offenders and how they operate to commit CEM crimes should be a priority in future training and support efforts (Leclerc et al., in preparation). It should be noted that knowledge transfer between police organisations nationally and internationally on how offenders operate to proceed with CEM activities is arguably a priority and can be facilitated by organisations, such as the ICMEC. It also seems imperative that police organisations keep investigators up to date with evolving technologies through training to facilitate the conduct of investigations online.

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

- Legislative and procedural requirements have also been reported as a challenge for online CEM investigators. Certain legislations often constrain their capacity to identify and apprehend CEM offenders online as covert investigators (see example under Point B above). Arguably, not only would streamlining legislative constraints be beneficial, but training and support on CEM legislation and procedural requirements may increase the capacity of investigators to speed their investigations in this context. Collaboration from prosecutors should also facilitate investigations, as much as possible, CEM investigations as investigators are always operating against time, which also puts at risk the safety of children. More research is needed to document how legislation impacts the efficacity of CEM investigations.

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

- Webpages are a key platform through which CEM is hosted and distributed. Westlake and Bouchard (2016) identified 10 CEM related networks comprising 4,831,050 websites by following hyperlinks on known sites. Despite the seemingly obvious risks associated with hosting CEM on webpages, many websites with such material do not

even attempt to avoid detection by masking the content or purpose (Westlake, Bouchard & Girodat 2017).

- Another common online platform for CEM distribution is P2P networks (Bissias et al., 2016; Bouhours & Broadhurst 2011; Krone et al., 2017; Wolak et al., 2011). Bissias et al. (2016) analysed five P2P networks and estimated that in December 2014 there were around 840,000 peers sharing CEM worldwide, with approximately three out of 10,000 internet users engaged in the distribution of CEM across these networks.

- While there is evidence of international distribution of CEM over P2P networks, much of the content may often be shared locally; Bouhours and Broadhurst (2011) found the ethnicity of CEM victims and perpetrators often reflected the perpetrator's country of origin.

- While it has been estimated that CEM constitutes a small percentage of all torrent traffic, it serves as a relevant investigative source for law enforcement as they can clearly identify the offender and observe their possession of illicit content (Borges et al., 2011; Layton & Watters, 2010). Though several tools provide investigators with unique capability to investigate CEM offenses along these lines, there is a key limitation with their functionality: they do not enable the identification of previously unidentified CEM. It is often difficult for law enforcement agencies to determine when new content has been released, as they must often identify it through manual analyses rather than hash value comparisons (Peersman et al., 2016). As a result, victims may go unrecognized for years and limit the potential for investigation into new abuse events.

- While websites and P2P networks are key sites of CEM distribution, other technologies are changing the landscape of CEM production and distribution (e.g., cloud storage, virtual reality, the Dark Web, live streaming; see Maxim et al. 2016). The Dark Web is arguably common for offenders heavily engaged in CEM activities and more aware of protecting their identify than most offenders. The Dark Web offers multiple layers of security for offenders to search for CEM content of interests, engage with like-minded offenders and even have access to real abuse content anonymously. While some offenders may not have the skills and knowledge to access and engage on the Dark Web, those who do can dramatically increase the consumption, distribution and production of CEM online for other offenders. In this context, there is a critical need to increase the capacity (and number) of online investigators through technological and human resources as well as training and knowledge transfer (e.g., social engineering, technology updates, sexual offenders and how they operate, CEM legislations, police investigation techniques, etc.).

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

- There is a vital role that the technology industry must play to limit the availability of CEM.

- Collaborations and partnerships exist that demonstrate tech companies' strategic efforts to reduce CEM, such as the implementation of scanning tools against websites to proactively identify CEM (e.g., Microsoft PhotoDNA). It is also clear that more can be

done to minimize abuse of services that facilitate the distribution of CEM, particularly by cloud storage providers who may enable storage of image and video content by offenders (Keller & Dance, 2019b). The same is true of social media companies whose services can be used to facilitate the direct or indirect production of CEM through youthful user profiles (Broadhurst, 2019).

- The technology industry has become an important player in proactive policing of CEM content through Open Web channels (Holt, 2018; Stambaugh et al., 2001; Wall, 2007). Though technology companies and service providers do not have constitutional powers to arrest individuals, but they are mandated by law under certain circumstances to protect their user base and comply with subpoenas and legal requests (Holt et al., 2017).

- Private industries may have greater access to unique data sets, technologies, and budgets than what may be available for law enforcement agencies.

- Different groups responsible for the investigation and policing of cyberspace can band together to increase their response capacity and regulatory power in ways that extend beyond what may be possible by traditional law enforcement agencies. In this respect, industry-based responses may be effective at the investigation of certain forms of cybercrimes, such as the production and distribution of CEM (Brenner, 2011).

- Network infrastructure providers, also known as Internet Service Providers (ISPs), can regulate behaviour through the contractual agreements with their clientele (Vincent-Jones, 2000; Wall, 2007). In fact, mobile service providers, web hosting services, cloud storage, and even social media services can be thought of as ISPs because they provide access to the Internet (Vincent-Jones, 2000; Wall, 2007). Customers are provided with terms and conditions arrangements, sometimes called Fair Use Policies (Holt & Bossler, 2016; Wall, 2007). The language within these contracts is guided by legal statutes at the local, state, or national level, and the ISP's own economic interests. They also communicate legal policies and requirements to users, particularly with respect to when and how user information may be given to law enforcement. However, it is unclear whether and to what extent customers take the time to read or understand ISP use policies, considering that many are used to distribute and share CEM. To that end, many search engines provide a warning banner when individuals enter in terms associated with CEM so as to notify the user that such content is illegal. The same is true for web hosting and social media service providers, such as Tumblr, Instagram, and Snapchat (Broadhurst, 2019; Keller & Dance, 2019a, 2019b).

- In the event that CEM is observed in a user account, whether by other users or law enforcement, they are encouraged to report that information to the ISP's security team (Holt, 2018; Wall, 2007). It is unclear how long the response to a complaint may take, or why problematic responses may be observed. For instance, Tumblr allows users to post image and video content that can be shared and liked by other users and has been used historically as an adult content sharing platform. Investigators who observed CEM through Tumblr accounts have reported the company has been extremely slow to respond to requests to take down user accounts or the CEM itself (Keller & Dance, 2019a, 2019b). In addition, several sites note that they will only provide information on offenses and cooperate with law enforcement when supplied with appropriate warrants and legal justifications.

- ISPs can also play a vital role in the formal investigation of CEM in coordination with law enforcement agencies (Wall, 2007). Individuals using P2P services to download CEM are actively violating their ISP terms of service. As a result, customer records may be subpoenaed or requested through search warrants when specific IP addresses they operate have attempted to download CEM through P2P networks (Wall, 2007). Additionally, ISPs can be subject to international laws despite having a fixed location in physical space as they may have users who reside in different nations with different laws and regulatory powers (Wall, 2007). This is particularly evident in CEM cases, where they may be subject to fines or criminal charges if it can be proven that they knowingly allowed their services to be used to host or distribute CEM content (Holt et al., 2017; Wall, 2007).

- Because of the harms presented by CEM and legal obligations to report this content, technology companies have developed strategies to proactively identify such content on their platforms. Companies like Microsoft and Facebook have produced tools that utilize algorithms to scan and hash media content and compare it to known hash values of CEM (Ehrenkranz, 2018). These programs can also use unique protocols to determine if known CEM content has been modified in some way so as to improve the identification of CEM (Langston, 2018). In turn, CEM content can be proactively deleted and used to produce investigative leads for corporate security and law enforcement. Not only do these tools increase the potential for proactive CEM detection, but they also minimize the need for human examination of content. Such efforts may help reduce the psychological and emotional stress placed on investigators to specifically examine CEM (e.g., Burruss et al., 2018; Seigfried-Spellar, 2018). In fact, Microsoft and Facebook have made their detection tools available to law enforcement so as to increase access to those who need these tools the most.

- The inherent benefit of such software is limited by the fact that they may only be used at specific times. For instance, some cloud storage providers indicate that they implement Microsoft's PhotoDNA tool to scan for CEM (Keller & Dance, 2019b). Recent reporting indicates that the tool is only implemented, however, when content is directly distributed from a user account which limits its ability to be used for proactive/preventative scanning (Keller & Dance, 2019b). Others, such as Amazon do not appear to implement these tools at any time. On the one hand, minimizing intrusive scanning is necessary to ensure user privacy and minimize the risk of false positive identification. On the other, these policies enable CEM content to be stored on their infrastructure without detection so long as the user does not proactively share content with others (Keller & Dance, 2019b).

- It is critical to note that gaining collaboration from social media platforms has been reported by investigators to be an important challenge during investigations. Some platforms may refuse to collaborate with investigators due to privacy laws, provided very limited evidence or at best, be very slow to respond to police enquiries. This all substantially impacts the quality of investigations and evidence. In many cases, the lack of collaboration from certain media makes it extremely difficult for investigators to follow a lead and arrest CEM offenders.

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

- There is a crucial overlap between child sexual abuse and CEM production. While the latter necessarily requires the former, the opposite is not true, and this is an important point for several reasons. There are similar individual and historical risk factors for child sexual abuse and CEM production and distribution. Different patterns of male and female involvement in CEM production also mirror, to some extent, gender differences in the modus operandi and motivations of male and female perpetrators of child sexual abuse (see, for example, Beech et al., 2009). The average age of perpetrators of CEM production and distribution approximates the average age of adult perpetrators of child sexual abuse (mid-adulthood; Lussier & Cale 2013). However, there are also unique risk factors that may drive CEM production aside from individual motivations specific to the abuse (sexual pleasure, power etc).

- CEM activities including production are typically conducted for the material itself (i.e., sexual gratification), which provides a link to contact offending. CEM production is also conducted for financial gain; material can be produced with ease, without having to get involved necessarily in organised crime or human trafficking, and without ever leaving the home. Finally, group status and engaging with like-minded offenders and communities are also important motivations to consider especially for offenders engaging in CEM activities on the Open and Dark Web (e.g., Holt, Blevins & Burkert 2010; Jenkins 2001; O'Halloran & Quayle 2010). It is well known that many offenders are seeking a high status in those communities by engaging actively in CEM activities, which may include administering sites and forums, providing advice on security matters, providing knowledge on how to sexually abuse children, and facilitating the access to, and distribution of, CEM. These motivations can all lead many offenders to contact offending for the first time.

- There are overlaps between offenders who produce and/or distribute CEM and those who engage in contact (sexual) offending (Bickart et al., 2019; Bissias et al., 2016; Bouhours & Broadhurst 2011; Gewirtz-Meydan et al., 2018; Krone & Smith 2017; Krone et al., 2017; McManus et al., 2015; Shelton et al., 2016; Wolak, Finkelhor, Mitchell & Jones 2011). McManus and colleagues (2015) found that CEM offenders (i.e., producers, distributors, and distributors/possessors) who had previously committed a sexual offence against a child were over seven times more likely to have produced CEM than those with no previous history of contact sexual offences. Krone and Smith (2017) and Krone et al. (2017) found that the production or provision of CEM, and being an administrator of a CEM network, were also associated with contact sexual offending.

- Although it is unclear how many offenders who initially engage only in the consumption and/or distribution of CEM on the Dark Web escalate to contact sexual offending, it is clear that some will turn to contact offending for different reasons, some as straight forward as sexual gratification, but others with the aim to perpetrate and record abuse to obtain other privileges in online CEM groups. Recording the abuse provides them with the opportunity to share real abuse content on the Dark Web in exchange for other privileges, such as gaining access to similar content (i.e., real abuse content) produced by other offenders and importantly, obtaining a higher status in CEM communities on the Dark Web (Leclerc et al., 2021b). The escalation from consuming and/or distributing CEM to contact offending is of particular concern as it arguably

generates CEM activities online (in the form of a cycle) as well as contact offending, putting the safety of children at greater risk of abuse.

G. Any related matters

- There is evidence that CEM investigators may experience adverse psychological outcomes (e.g., secondary traumatic stress, burnout) due to the nature of these investigations (Burruss, Holt & Wall-Parker 2018; Perez et al. 2010; Seigfried-Spellar 2018).

- Powell, Cassematis, Benson, Smallbone and Wortley (2015) examined investigators' perceptions of their reactions to viewing CEM content. The results indicated that CEM investigators experience significant emotional, cognitive, social and behavioural consequences as a result of viewing CEM. The study indicated that the degree of negative consequences varies markedly across individuals, types and content of material and viewing context (with variation also based on individual, case-related and contextual factors). In terms of specific consequences, many participants reported short-term reactions of disgust and anger and long-term reactions reflecting anger as the dominant emotional response. Other symptoms reported by participants included secondary traumatic stress disorder (e.g., intrusive imagery, flashbacks, nightmares and social withdrawal), increased generalised distrust of people, over protectiveness of children and difficulty in relationships with partners and children. At the international level, investigators reported higher emotional fatigue, burnout, and secondary trauma due to their exposure to CEM content (e.g., Burruss et al., 2018; Perez et al., 2010). Consistent with their role, participants also described desensitisation to viewing CEM. Importantly, the experience of these negative consequences has also been reported in the broader sexual offending literature by therapists working with sexual offenders (e.g., Elias and Haj-Yahia, 2016). There is also higher emotional fatigue, burnout, and secondary trauma reported by investigators due to their exposure to CEM content (e.g. Burruss et al., 2018; Perez et al., 2010).

- Online CEM investigators also reported the need for mental health/psychological and wellbeing support (55%) as well as training on coping mechanisms and emotional intelligence/resilience related to working in the field of child sexual exploitation online (24%) (Leclerc et al., in preparation). Even though some investigators may not feel the immediate need for psychological support and training on emotional resilience related to CEM, it remains pertinent to provide more opportunities for investigators to benefit from support and undertake training to protect their wellbeing and prevent the accumulation of negative consequences on their mental health that may lead to more serious problems. This is essential since the workforce of online CEM investigators is very specialised and currently operating with very limited human resources (i.e., low numbers of investigators) in a field that involves many complex challenges (discussed above).

- It is important to acknowledge that the information provided in this submission is primarily focused on research and policy information emerging from Western Industrialized nations. At present, the majority of research and policy related to CEM seems to originate from these nations. Access to the Internet and technology varies dramatically by region and country at the international level, particularly as a function of poverty and regulation of Internet connectivity (Holt & Bossler, 2016). At the same

time, there is evidence that CEM production on a fee-for-service basis originates from Southeast Asian nations due in part to high levels of poverty (Broadhurst, 2019). An increase in online streaming of child sexual exploitation for financial gain in developing countries has also been observed due in part the expanding reach of 4G, and recently 5G. Thus, crucial research is needed to investigate the state of CEM production, distribution, and prevention efforts in non-Western contexts. Such insights are essential to better link law enforcement efforts around the world and assess the ways that industry bodies are actively engaging in countries with limited access to technology.

- It might be beneficial for academia to scientifically evaluate CEM investigation and takedown strategies, regardless of their origin with law enforcement or industry (Holt, 2018; Holt et al., 2015). Understanding the cost to implement a strategy and map its impact on offender displacement and CEM distribution is important to understand its utility in the field. In addition, research on assessing the impact of various CEM investigative methods on investigators to improve the mental and physical health of law enforcement officials over time could prove insightful for training and support purposes (Burruss et al., 2018; Holt et al., 2015).

References

Aldridge, J., & Askew, R. (2017). Delivery dilemmas: How drug cryptomarket users identify and seek to reduce their risk of detection by law enforcement. *International Journal of Drug Policy, 41,* 101–109.

Aldridge, J., Stevens, A., & Barratt, M. J. (2018). Will growth in cryptomarket drug buying increase the harms of illicit drugs? *Addiction, 113,* 789–796.

Andress, J., & Winterfeld, S. (2013). *Cyber warfare: Techniques, tactics, and tools for security practitioners* (2nd ed.). Waltham MA: Syngress.

Beech, A. R., Parrett, N., Ward, T., & Fisher, D. (2009). Assessing female sexual offenders' motivations and cognitions: an exploratory study. *Psychology, Crime & Law, 15*, 201–216.

Bickart, W., McLearen, A. M., Grady, M. D., & Stoler, K. (2019). A descriptive study of psychosocial characteristics and offense patterns in females with online child pornography offenses. *Psychiatry, Psychology and Law, 26,* 295–311.

Bissias, G., Levine, B., Liberatore, M., Lynn, B., Moore, J., Wallach, H., & Wolak, J. (2016). Characterization of contact offenders and child exploitation material trafficking on five peer-to-peer networks. *Child Abuse & Neglect, 52,* 185–199.

Borges, R., Houssain, K., Patton, R., & Masal, Y. (2011). *BitPredator: A Discovery Algorithm for BitTorrent Initial Seeders and Peers. International Conference on Advanced Computer Theory and Engineering. 4th (ICATE 2011).* ASME Press. https://ebooks.asmedigitalcollection.asme.org/content.aspx?bookid=487&sectionid=38793947.

Bouhours, B., & Broadhurst, R. (2011). *On-line child sex offenders: Report on a sample of peer-to-peer offenders arrested between July 2010 – June 2011*. Canberra: Australian National University.

Brenner, S. W. (2011). Defining cybercrime: A review of federal and state law. In R. D. Clifford (Ed.). *Cybercrime: The investigation, prosecution, and defense of a computer-related crime* (pp. 15–104). (3rd ed.). Raleigh, NC: Carolina Academic Press.

Broadhurst, R. (2019). Child sex abuse images and exploitation materials. Child sex abuse images and exploitation materials. In R. Leukfeldt, & T. J. Holt (Eds.). *Cybercrime: The human factor*. London: Routledge.

Brown, R., Napier, S. & Smith, R. (2020). Australians who view live streaming of child sexual abuse: An analysis of financial transactions. *Trends & Issues in Crime and Criminal Justice*. (no 589). Canberra: Australian Institute of Criminology.

Burruss, G. W., Holt, T. J., & Wall-Parker, A. (2018). The hazards of investigating internet crimes against children: Digital evidence handlers' experiences with vicarious trauma and coping behaviors. *American Journal of Criminal Justice, 43,* 433–447.

Bursztein, E., Clarke, E., DeLaune, M., Eliff, D. M., Hsu, N., Olson, L., Shehan, J., Thakur, M., Thomas, K., & Bright, T. (2019). *Rethinking the detection of child sexual abuse imagery on the internet.* In the World Wide Web Conference (pp 2601–2607). https://doi.org/10.1145/3308558.3313482.

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.

Copeland, C., Wallin, M. & Holt, T. J. (2020). Assessing the practices and products of darkweb firearm vendors. *Deviant Behavior, 41*, 949–968.

Cox, J. (2016, July 27). Dozens of lawyers across the US fight the FBI's mass hacking campaign. *Motherboard by vice*. https://www.vice.com/en_us/article/aek4ak/dozens-of-lawyers-across-the-us-fight-the-fbis-mass-hacking-campaign-playpen.

Egmont Group of Financial Intelligence Units. (2020). *Combatting child sexual abuse and exploitation through financial intelligence*. Public Bulletin. July.

Ehrenkranz, M. (2018, October 24). Facebook is using new AI tools to detect child porn and catch predators. *Gizmodo.* https://gizmodo.com/facebook-is-using-new-ai-tools-to-detect-child-porn-and-1829968486.

Elias, H., & Haj-Yahia, M. (2016). On the lived experience of sex offenders' therapists: Their perceptions of intrapersonal and interpersonal consequences and patterns of coping. *Journal of Interpersonal Violence, 34*, 1-25.

Erdely, R., Kerle, T., Levine, B., Liberatore, M., & Shields, C. (2010). Forensic investigation of peer-to-peer file sharing network. *Proceedings of the Digital Forensics Research Workshop Conference (DFRWS),* Portland, OR.

Fennelly, J. E. (1991). Refinement of the inevitable discovery exception: The need for a good faith requirement. *William Mitchell Law Review, 17*(4), 1085–1109.

Ferraro, M. M., Casey, E., & McGrath, M. (2005). *Investigating child exploitation and pornography: The Internet, the law and forensic science.* Burlington, MA: Elsevier.

Fortin, F., Paquette, S., & Dupont, B. (2018). From online to offline sexual offending: Episodes and obstacles. *Aggression and Violent Behavior, 39,* 33–41.

Franqueira, V. N. L., Bryce, J., Mutawa, N. A., & Marrington, A. (2018). Investigation of indecent images of children cases: Challenges and suggestions collected from the trenches. *Digital Investigation, 24*, 95–105.

Garcha, R. K. (2018). NITS a no-go: Disclosing exploits and technological vulnerabilities in criminal cases. *New York University Law* Review (pp. 822–863).

Gewirtz-Meydan, A., Walsh, W., Wolak, J. & Finkelhor, D. (2018). The complex experience of child pornography survivors. *Child Abuse & Neglect, 80,* 238–248.

Harkin D., Whelan, C., & Chang, L. (2018). The challenges facing specialist police cyber-crime units: An empirical analysis. *Police Practice and Research: An International Journal, 19*(6), 519–536.

Holt, T. J. (2018). Regulating cybercrime through law enforcement and industry mechanisms. *The Annals of the American Academy of Political and Social Science, 679*(1), 140–157.

Holt, T. J., Blevins, K. R., & Burkert, N. (2010). Considering the pedophile subculture online. *Sexual Abuse, 22,* 3–24.

Holt, T. J., & Bossler, A. M. (2016). *Cybercrime in progress: Theory and prevention of technology-enabled offenses*. London: Routledge.

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2017). *Cybercrime and digital forensics: An introduction.* London: Routledge.

Holt, T. J., Burruss, G. W., & Bossler, A. M. (2015). *Policing cybercrime and cyberterror*. Raleigh, NC: Carolina Academic Press.

Holt, T. J., Cale, J., Leclerc, B., & Drew, J. (2020). Assessing the challenges affecting the investigative methods to combat CEM offenses. *Aggression & Violent Behavior, 55*. https://doi.org/10.1016/j.avb.2020.101464.

Holt, T. J., & Dupont, B. (2019). Exploring the factors associated with rejection from a closed cybercrime community. *International journal of offender therapy and comparative criminology, 63*(8), 1127–1147.

Hoydal, H. F., Stangvik, E. O., & Hansen, N. R. (2017). Breaking the Dark Net: Why the police share abuse pics to save children. *VG17 October*. www.vg.no/spesial/2017/undercover-darkweb/.

Hutchings, A., & Holt, T. J. (2015). A crime script analysis of the online stolen data market. *British Journal of Criminology, 55,* 596–614.

International Center for Missing and Exploited Children. (2017). *Commercial child pornography: A brief snapshot of the Financial Coalition Against Child Pornography.* http://www.icmec.org/wp-content/uploads/2016/09/FCACPTrends.pdf.

International Centre for Missing & Exploited Children and Standard Chartered (2021). *Cryptocurrency and the Trade of Online Child Sexual Abuse Material.* Published by The International Centre for Missing & Exploited Children. www.icmec.org

Internet Watch Foundation. (2017). *About us.* https://www.iwf.org.uk/about-iwf.

Internet Watch Foundation. (2018). *Once upon a year*. Cambridge, UK: IWF.

Internet Watch Foundation (2019). *Trends in online child sexual exploitation: examining the distribution of captures of live-streamed child sexual abuse*. May. Cambridge, UK: IWF.

Jenkins, P. (2001). *Beyond tolerance: Child pornography on the internet*. New York: New York University Press.

Joh, E. (2009). Breaking the law to enforce it: Undercover police participation in crime. *Stanford Law Review, 62,* 239–273.

Keller, M. H., & Dance, G. J. X. (2019a). *The internet is overrun with images of child sexual abuse. What went wrong?* The New York Times. September 28. https://www.nytimes.com/interactive/2019/09/28/us/child-sex-abuse.html.

Keller, M. H., & Dance, G. J. X. (2019b). *Child abusers run rampant as tech companies look the other way*. The New York Times. September 29. https://www.nytimes.com/interactive/2019/11/09/us/internet-child-sex-abuse.html.

Kloess J.A., Hamilton-Giachritsis, C.E., & Beech, A. (2019). Offense processes of online sexual grooming and abuse of children via Internet communication platforms. *Sexual Abuse: A Journal of Research and Treatment, 31*, 73-96.

Kloess J.A., Smith, S.S., Hamilton-Giachritsis, C.E., Long, M.L., Shipley, D., & Beech, A. (2017). A qualitative analysis of offenders' modus operandi in sexually exploitative interactions with children online. *Sexual Abuse: A Journal of Research and Treatment, 29*, 563-591.

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

Krone, T., Smith, R. G., 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.

Langston, J. (2018). How PhotoDNA for Video is being used to fight online child exploitation (2011) In E. R. Larence (Ed.). *Combating child pornography: Steps are needed to ensure that tips to law enforcement are useful and forensic examinations are cost effective*. Washington DC: DIANE Publishing.

Layton, R., & Watters, P. (2010). Investigation into the extent of infringing content on BitTorrent networks. *Internet Commerce Security Laboratory*, 8–10.

Leclerc, B. (2017). Boosting Crime Scene Investigations Capabilities through Crime Script Analysis. In Rossy, Q., Decary-Hetu, D., Delemont, O., & Mulone, M. (eds.), *Routledge Handbook of Forensic Criminology*. UK: Routledge.

Leclerc, B. & Cale, J. (2015). Adult sexual offenders in youth-oriented institutions: Evidence on sexual abuse victimizations experiences of offenders and their offending patterns. *Trends and Issues in Crime and Criminal Justice. (*No 497). Canberra: Australian Institute of Criminology.

Leclerc, B., Cale, J., Holt, T., & Drew, J. (in preparation). *Child Sexual Abuse Material Online: The Perspective of Online Investigators on Training and Support.*

Leclerc, B., Drew, J., Holt, T., Cale, J., & Singh, S. (2021a). 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.

Leclerc, B., Drew, J., Holt, T., & Cale, J. (2021b). *Child sexual abuse material on the darknet: A script analysis*. Confidential report for Law Enforcement. Australian Institute of Criminology's CSAM Reduction Research Program. Canberra: Australian Institute of Criminology.

Leclerc, B., Proulx, J. & Beauregard, E. (2009). Examining the modus operandi of sexual offenders against children and its practical implications. *Aggression and Violent Behavior, 14*, 5-12.

Leclerc, B. Smallbone, S. & Wortley, R. (2013). Interpersonal scripts and victim reaction in child sexual abuse: A quantitative analysis of the offender-victim interchange. In Leclerc, B. and Wortley, R. (eds.) *Cognition and crime: Offender decision-making and script analyses*. Crime Science Series, London, UK: Routledge.

Leclerc, B., Wortley, R. & Smallbone, S. (2011). Getting into the script of adult child sex offenders and mapping out situational prevention measures. *Journal of Research in Crime and Delinquency, 48*, 209-237.

Lee, J. R., & Holt, T. (2020). The challenges and concerns of using big data to understand cybercrime. In B Leclerc & J Cale (eds), *Big Data: Criminology at the edge*. UK: Routledge, 85–103.

Lee, J. R., Holt, T. J., Burruss, G. W., & Bossler, A. M. (2019). Examining English and Welsh Detectives' Views of Online Crime. *International Criminal Justice Review*, *31*(1), 20–39. https://doi.org/10.1177/1057567719846224.

Lussier, P., & Cale, J. (2013). Beyond sexual recidivism: A review of the sexual criminal career parameters of adult sex offenders. *Aggression and Violent Behavior, 18,* 445–457.

Martin, J., Munksgaard, R., Coomber, R., Demant, J., & Barratt, M. J. (2020). Selling drugs on darkweb cryptomarkets: Differentiated pathways, risks and rewards. *British Journal of Criminology, 60*, 559–578.

Maxim, D. J. A., Orlando, S. M., Skinner, K. L., & Broadhurst, R. G. (2016). *Online child exploitation material: Trends and emerging issues.* Canberra: Australian National University Cybercrime Observatory and Office of the Children's e-Safety Commissioner.

McManus, M. A., Long, M. L., Alison, L., & Almond, L. (2015). Factors associated with contact child sexual abuse in a sample of indecent image offenders. *Journal of Sexual Aggression, 21,* 368–384.

National Center for Missing and Exploited Children. (2017). *FAQs.* www.missingkids.com/Missing/FAQ.

O'Halloran, E., & Quayle, E. (2010). A content analysis of a "boy love" support forum: Revisiting Durkin and Bryant. *Journal of Sexual Aggression, 16,* 71–85.

Peersman, C., Schulze, C., Rashid, A., Brennan, M., & Fischer, C. (2016). iCOP: Live forensics to reveal previously unknown criminal media on P2P networks. *Digital Investigation, 18,* 50–64.

Perez, L. M., Jones, J., Englert, D. R., & Sachau, D. (2010). Secondary traumatic stress and burnout among law enforcement investigators exposed to disturbing media images. *Journal of Police and Criminal Psychology, 25,* 113–124

Prat, S., Bertsch, I., Chudzik, L., & Réveillère, C. (2014). Women convicted of a sexual offence, including child pornography production: Two case reports. *Journal of Forensic and Legal Medicine, 23,* 22–24.

Reid, J. A. (2016). Entrapment and enmeshment schemes used by sex traffickers. *Sexual Abuse: A Journal of Research and Treatment, 28,* 491–511.

Seigfried-Spellar, K. C. (2018). Assessing the psychological well-being and coping mechanisms of law enforcement investigators vs. digital forensic examiners of child pornography investigations. *Journal of Police and Criminal Psychology, 33*, 215–226.

Seto, M., Buckman, C., Dwyer, R. G., & Quayle, E. (2018). *Production and active trading of child sexual exploitation images depicting identified victims.* National Center for Missing and Exploited Children. https://www.missingkids.org/content/dam/missingkids/pdfs/ncmec-analysis/Production%20and%20Active%20Trading%20of%20CSAM_FullReport_FINAL.pdf.

Sheehan, V., & Sullivan, J. (2010). A qualitative analysis of child sex offenders involved in the manufacture of indecent images of children. *Journal of Sexual Aggression*, *16*, 143–167.

Shelton, J., Eakin, J., Hoffer, T., Muirhead, Y., & Owens, J. (2016). Online child sexual exploitation: An investigative analysis of offender characteristics and offending behavior. *Aggression and Violent Behavior, 30,* 15–23.

Stambaugh, H., Beaupre, D. S., Icove, D. J., Baker, R., Cassady, W., & Williams, W. P. (2001). *Electronic crime needs assessment for state and local law enforcement*. Washington, DC: National Institute of Justice, U. S. Department of Justice.

Vendius, T. T. (2015). Proactive undercover policing and sexual crimes against children on the internet. *The European Review of Organised Crime, 2,* 6–24.

Vincent-Jones, P. (2000). Contractual governance: Institutional and organizational analysis. *Oxford Journal of Legal Studies, 20,* 317–351.

Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age.* Cambridge: Polity Press.

Weaver, N. (2016). The end of the NIT. *Lawfare.* (5 December 2016). https://www.lawfareblog.com/end-nit.

Westlake, B. G. (2020). The past, present, and future of online child sexual exploitation: Summarizing the evolution of production, distribution, and detection. In T Holt & A Bossler (eds), *The Palgrave handbook of international cybercrime and cyberdeviance*. New York: Palgrave Macmillan: 1225–1253.

Westlake, B. G., & Bouchard, M. (2016). Liking and hyperlinking: Community detection in online child sexual exploitation networks. *Social Science Research, 59,* 23–36.

Westlake, B. G., Bouchard, M., & Girodat, A. (2017). How obvious is it? The content of child sexual exploitation websites. *Deviant Behavior, 38,* 282–293.

Widenhouse, K. C. (2017). Playpen, the NIT, and Rule 41(b): Electronic "searches" for those who do not wish to be found. *Journal of Business & Technology Law, 13(*1), 143–169.

Wolak, J., Finkelhor, D., & Mitchell, K. (2011). Child pornography possessors: Trends in offender and case characteristics. *Sexual Abuse: A Journal of Research and Treatment, 23*, 22–42.

Wolak, J., Finkelhor, D., Mitchell, K., & Jones, L. M. (2011). Arrests for child pornography production: Data at two time points from a national sample of U.S. law enforcement agencies. *Child Maltreatment,* 16, 184–195.