AFP
AUSTRALIAN FEDERAL POLICE

Parliamentary Joint Committee on Law Enforcement

Inquiry into the *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019*

22 October 2021

Submission by the Australian Federal Police

Introduction

1. The Australian Federal Police (AFP) welcomes the opportunity to make a submission to the Parliamentary Joint Committee on Law Enforcement (the Committee) inquiry into the *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019* (the AVM Act).
2. The live streaming and wide spread sharing of the abhorrent material created by the Christchurch terrorist attack demonstrated the potential for live streaming, video sharing, and social media platforms to be exploited by perpetrators to amplify extremist messaging in the immediate and long term aftermath of their offending.
3. The AVM Act was introduced to address gaps in Australia's legislative framework to require internet, hosting and content services to proactively take action to address abhorrent violent material accessible through their services as soon as it is identified. The AFP was consulted during the development of this legislation, which aims to ensure such platforms cannot be exploited or weaponised by perpetrators of violence.
4. This submission focuses on the AFP's operational experience in combatting abhorrent violent material both in the context of the AVM Act and relevant criminal conduct more broadly. We recommend it be read alongside submissions from the Department of Home Affairs, Attorney-General's Department and Office of the eSafety Commissioner to provide the full context of the Commonwealth's response to abhorrent violent material online.

Threat Environment

Online Offending

5. The AFP has identified increasing criminal use of the internet – both on the clear and dark web. The internet is used to facilitate all serious crime types, but particularly terrorism and violent extremism, child exploitation, trafficking of illicit substances and firearms, and the propagation of malware and stolen personal identification.
6. The continued and increasing adoption of online communication platforms allows for the instantaneous sharing of abhorrent and malicious content to international audiences. The ability for individuals to rapidly disseminate such content and store it across disparate platforms and jurisdictions allows extremist messaging and abhorrent violent material to duplicate in such a way that removing the source content can have limited impact.
7. Law enforcement agencies face significant challenges in addressing this threat, noting technological advancements, international jurisdiction considerations and the speed at which information and material can be propagated across new and varied platforms. The harm posed to the Australian community continues to grow.

Terrorism

8. The 15 March 2019 live streaming of two mass shooting terrorist attacks at the Al Noor Mosque and Linwood Islamic Centre in Christchurch, New Zealand demonstrated how

live streaming capabilities could be utilised by perpetrators to amplify their extremist messaging.

9. Within Australia, the terrorism threat level remains PROBABLE, as credible intelligence indicates that individuals or groups have the intent and capability to conduct a terrorist attack in Australia. The ease of access and wealth of extremist material online has broadened its reach to mainstream audiences, accelerating the process of radicalisation.

10. Online platforms significantly expand the audiences targeted by extremists, and provide an accessible platform for radicalisation and recruitment. Increasingly, violent extremists across all ideological spectrums exploit this capability to spread extreme and harmful propaganda, seed division and garner support for their cause.

11. During the COVID-19 pandemic, the AFP has identified extremists taking advantage of isolation, loneliness and financial stress to boost their numbers. While the AFP has observed additional visitors to online extremist forums, this has not yet translated to an identifiable change in medium to long-term membership.

Child Exploitation

12. The AFP continues to see high volumes of reports relating to online child abuse material in Australia. In 2020-21 22,600 incoming reports of child exploitation were received by the Australia Centre for Countering Child Exploitation (ACCCE).

13. The borderless nature of this offending, along with advances in technology and evolving methodologies means that despite decades of effort, the exploitation of children has expanded across the globe and out-paced every attempt to respond.

14. Further, current limitations in international travel and the perception that the consumption of material online is likely to be detected by law enforcement, have contributed to a significant demand for the consumption of Live Online Child Sexual Abuse (LOCSA), also known as 'Live Distance Child Abuse'.

15. LOCSA is a trend being observed within the child exploitation space that is primarily executed through livestreaming, with no electronic trace left on the device or remote servers barring session logs or data usage statistics. As a result, law enforcement often are only alerted to the crime where the offender captures and uploads screenshots or video to other platforms. Where detected, providers hosting LOCSA may be subject to the AVM Act.

16. The AFP is also aware of another emerging trend being observed by the ACCCE which is called 'capping', where an offender portrays themselves through an assumed, approachable identity (such as another child) to engage directly with a child. Offenders will use social media and communications platforms that support picture and video distribution and streaming to groom children into live-streaming sexual acts whilst they record. A single offender can produce a high number of child abuse videos and victims. Offenders may manipulate a victim into producing additional material or abusing another child, such as a sibling.

Role of the AFP

17. To date, the AFP has received **13** reports relating to abhorrent violent material identified online. The material consisted of **6** instances of terrorism related material, **1** instance of rape, **1** instance of murder, **1** instance of child abuse material, and **1** instance of criminal activity. These reports were then referred to the eSafety Commissioner for issuing a takedown notice with the internet provider or platform.

18. There were **3** referrals received by the AFP and reviewed by the eSafety Commissioner which were determined not to be 'abhorrent violent material', and the matters were returned to the platforms for further investigation as online behavioural violations.

19. Following the commencement of the AVM Act, the AFP established Operation HAFNON to coordinate the agency's approach to the new legislation. As part of Operation HAFNON, an Incident Coordination Centre (ICC) was activated on 5 April 2019 operating between 8am and 8pm each day. The ICC was deactivated on 12 April 2019, and responsibility for coordinating the AFP's response was subsumed by the AFP's National Operations State Service Centre (NOSSC).

NOSSC

20. The AFP NOSSC has a key coordination role in the AFP's initial response to incidents. The NOSSC is the single contact point, 24 hours a day, for AFP and other agency operations and crisis centres. It maintains a situational awareness of critical or significant events and briefs the AFP Commissioner and Senior Executive on these events.

21. In the event of a major incident, the NOSSC will coordinate the AFP's initial response with these centres. Where an incident involves AVM, the NOSSC will coordinate the AFP's response. If the underlying conduct is a Commonwealth offence, the NOSSC will refer the material to the relevant AFP area for investigation (for example, Counter Terrorism Command where the underlying conduct is a terrorist act). Where the underlying conduct is a State or Territory offence, the NOSSC will refer the material to one or more relevant State/Territory Police.

22. Where there are international elements to the underlying conduct, the NOSSC may refer to relevant countries via INTERPOL. There may be instances where material falls within ASIO's remit and is referred to them.

Child Protection Operations and ACCCE

23. The AFP, through the ACCCE and the AFP-led online child safety initiatives and programs, lead law enforcement focused crime prevention and deterrence initiatives to counter online child sexual exploitation.

24. The ACCCE's Child Protection Triage Unit (CPTU) receive the vast majority of the reports of online Child Exploitation. These reports can originate from a variety of sources, though most are received from the National Centre for Missing and Exploited Children (NCMEC) in the United States. These reports contain information regarding the uploading and sharing of child abuse material on US-based platforms.

25. Other reports received by CPTU are made by members of the public, predominantly parents or carers reporting that their child has been groomed and exploited online or the

reporting of online links that contain child abuse material. The remaining reports are received from foreign law enforcement agencies, Australian-based government departments, or private organisations.

26. Every day CPTU triages each report that is received. These reports are assessed to ascertain whether they meet the threshold for investigation by the Joint Anti-Child Exploitation Teams (JACETs), including whether they contain an Australian offence and enough information or identifiers to investigate the matter further.

27. If these criteria are met, the reports are worked up to clearly identify the person of interest and where they are located. The matter is provided to the JACETs for investigation.

Australian Taskforce to Combat Terrorist and Extreme Violent Material Online

28. On 26 March 2019, the Prime Minister chaired a Summit in Brisbane which the AFP attended to discuss Australian Government and industry responses to the sharing of content related to the Christchurch terrorist attack. A key outcome of the Summit was the establishment of the Taskforce to Combat Terrorist and Extreme Violent Material Online (the Taskforce).

29. Comprising law enforcement, government and industry representatives, the Taskforce examined the use of the internet by terrorist and violent extremists to provide advice to Government on practical, tangible and effective measures and commitments to combat the upload and dissemination of terrorist and extreme violent material. The AFP was proud to actively participate in the Taskforce.

30. The Taskforce published its report in June 2019, with 30 recommendations. These included measures to enhance transparency reporting by platforms, to create a 24/7 government response capability, and for the eSafety Commissioner to direct Australian internet service providers to block terrorist and violent extremist material in limited circumstances.

Other Legislative measures available to the AFP to combat abhorrent material online

31. The AFP is constantly working to combat and prevent Australian telecommunications networks and facilities being used in, or in relation to, the commission of offences against Commonwealth or State and Territory legislation.

32. Section 313(3) of the Telecommunications Act 1997 requires carriers and carriage service providers to assist officers and authorities of the Commonwealth, and of the States and Territories, as is reasonably necessary for particular purposes. These include enforcing the criminal law and imposing pecuniary penalties, assisting the enforcement of the criminal laws in force in a foreign country; assisting in investigation and prosecution of crimes within the International Criminal Court Act and International War Crimes Tribunal, protecting the public revenue and safeguarding national security.

33. The AFP has previously submitted requests under the Access Limitation Scheme (ALS) regarding INTERPOL's 'worst of' list of websites containing child abuse material in accordance with subsection 313(3) of the Telecommunications Act.

34. The ALS commenced on 30 June 2011 and operates at the internet service provider domain name server level. INTERPOL compiles a 'worst of' list of websites (the list) which have been identified, assessed and determined as containing the most severe child exploitation material. The criteria utilised by INTERPOL for inclusion of a domain in this list means that the subject material is considered child exploitation material under all Australian legislation.

35. The use of section 313(3) nevertheless remains available when seeking the assistance of carriers and carriage service providers and remains a valid authority where preventative action or disruptive action is requested without any intention to seek access to information to support further investigative or prosecutorial action.

Engagement with Partners

Office of the eSafety Commissioner

36. The AFP and the eSafety Commissioner have a close and long-standing relationship, working collaboratively on a range of issues relating to online child protection, including the prevention of technology-enabled crimes through education and awareness programs and initiative.

37. The eSafety Commissioner is empowered under the AVM Act to issue a notice to a content service or hosting service provider notifying them that their service can be used to access or host abhorrent violent material. The AFP may liaise with the eSafety Commissioner to determine whether it is appropriate for the eSafety Commissioner to issue a notice to remove and in addition to this whether the AFP will commence an investigation or prosecution (noting that a prosecution can be commenced without issuing a notice). Any further failure to remove and report may be referred to the AFP.

38. The AFP and the eSafety Commissioner (eSafety) work collaboratively on a range of matters relating to child protection, including the reporting and referral of online child sexual exploitation material and the prevention of cyber-related crimes through education and awareness initiatives.

39. The AFP and eSafety Commissioner signed a (revised) Memorandum of Understanding (MoU) in September 2020, with the aim of clarifying agency remit and reducing duplication on child protection matters.

40. The working relationship and arrangements under the MoU have been productive, including fortnightly meetings at the working level to discuss initiatives relating to prevention and communications.

41. The eSafety Commissioner is a current member of the AFP led-ACCCE Board of Management and the agency is a key partner in supporting strategic initiatives towards preventing online child sexual exploitation.

Industry

42. The AFP collaborates with partners across government and Commonwealth agencies, law enforcement and investigative authorities, non-government organisations, the private sector, and academia to keep Australians safe. Relationships with industry often form

the basis for information sharing which enhance investigations and protect Australians from harm. This is recognised in the AFP's '2020 and Beyond' Strategy, which reaffirmed our commitment to engaging with industry and investing in partnerships to maximise our capacity to keep Australians safe.

43. The ACCCE has a strong relationship with many social media platforms such as Facebook, Google, WhatsApp, Snapchat, and Twitter at a practitioner level, which expedites flow of information.

44. These platforms also report to the NCMEC, where the content is triaged and sent to the ACCCE CPTU for examination and provision to law enforcement agencies. The AFP also has a NCMEC in-house position to provide a dedicated 'value-add' to reports and help support the referral process.

45. We recognise the need for genuine and valuable partnerships with industry, noting their critical role in the prevention and disruption of crime online (particularly child exploitation). Their support is essential to any effective framework for controlling the spread of abhorrent violent material online.

The Abhorrent Violent Material Framework

46. Broadly, the AVM Act created two new offences for internet service providers and content or hosting service providers by:

    - Criminalising platforms located anywhere in the world that do not notify the AFP within a reasonable time of them becoming aware their service is providing access to enable the streaming of abhorrent violent conduct that is happening in Australia.
    - Criminalising the failure to remove abhorrent violent material expeditiously.

47. The scope of the offences are limited to very specific categories of the most violent audio-visual material produced by the perpetrator of the abhorrent violent conduct or their accomplice.

The scope of the framework

48. The existing definition of 'abhorrent violent material' captures the recording or streaming of actual acts of murder, rape, torture and terrorism involving physical harm and/or violent kidnapping. The Act specifically targets the availability of of abhorrent violent material by content, internet and hosting providers, but does not cover ordinary possession.

49. As flagged in our recent submission to the Parliamentary Joint Committee on Intelligence and Security *inquiry into extremist movements and radicalism in Australia,* the AFP is aware of the serious consequences caused by the possession, viewing, sharing and distribution of material (including images and written content) relating to extremist ideology. This can include images and videos of executions by immolation, firing squad or beheading as well as rapes linked to terrorist organisations and religious ideologies. This content would fall within the definition of abhorrent violent material.

50. The existing Commonwealth Criminal Code sections 101.4 and 101.5 make it an offence to possess things connected with terrorist acts and collect or make documents likely to facilitate terrorist acts. They require a connection to preparation for, engagement in, or assistance in a terrorist act, and are targeted towards offending at the higher end of criminal activity.

51. These offences cannot always adequately address the type of criminal activity seen in the current threat environment, where the viewing of extremist material circulated online acts as a precursor or catalyst for acts of terrorism. The AFP has observed that the majority of abhorrent violent material identified in the possession of, or shared and received by, a person of interest is not subject to any relevant offences currently covered under Commonwealth or local legislation.

52. As a result, there is a legislative gap to pursing individuals who simply possess or disseminate abhorrent violent material or extremist material that does not fall within the scope of existing offences. This impedes the ability for investigators to disrupt individuals and small groups at an early stage in the attack planning continuum, and requires officers to view images and videos likely to cause distress with no path towards charging.

Conclusion

53. The use of live streaming, video sharing, and social media platforms to spread abhorrent violent material continues, and through the anonymity and accessibility offered online, poses ongoing challenges to law enforcement.

54. The AFP would be pleased to expand on these issues at a public hearing.