Australian Government
Department of Home Affairs

Department of Home Affairs Submission to the Inquiry into the Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019

Parliamentary Joint Committee on Law Enforcement

15 October 2021

Table of Contents

Introduction

The Department of Home Affairs (the Department) has lead policy responsibility for online terrorism and violent extremism, including the policy underpinning the Abhorrent Violent Material amendments to the Commonwealth *Criminal Code Act 1995*. As such, the Department welcomes the opportunity to make a submission to the Parliamentary Joint Committee on Law Enforcement's (the Committee) inquiry into the *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019* (the AVM Act).

The Christchurch terrorist attack took place on 15 March 2019. 51 people were killed and 50 injured, and the 17 minute live stream of the attack was viewed some 4,000 times before being removed. The attack demonstrated the potential for live streaming, video-sharing, and social media platforms to be exploited by terrorists and extremists to amplify their actions and messages, and highlighted the challenges faced by government and law enforcement in responding to terrorist and violent extremist content online.

The Australian Parliament swiftly passed the AVM Act, which came into effect on 6 April 2019, to address gaps in Australia's legislative framework.

The AVM Act was introduced to protect Australians from the livestreaming of violent content, and to reduce the incidence of live streaming, video sharing and social media platforms being exploited or weaponised by perpetrators of violence. To this end, the Act seeks to ensure that internet, hosting and content service providers (IHCSPs) expeditiously remove or cease hosting AVM on their services, and refer AVM to the Australian Federal Police (AFP) where they suspect that the abhorrent violent conduct depicted in the AVM occurred, or is occurring, in Australia.

We recommend this submission be read alongside the submissions from the AFP, Attorney-General's Department and the eSafety Commissioner, to provide the full context of the Commonwealth's response to abhorrent violent material online.

Abhorrent Violent Material

AVM is recorded or streamed audio, visual or audio-visual material of a person engaging in: a terrorist act (involving physical harm or the death of another person), murder or attempted murder, torture, rape, or violent kidnapping (including threat of violent kidnapping). This material must be recorded or streamed by a perpetrator or their accomplice.

AVM is limited to material exclusively capturing the most egregious of offences. The specific violent conducts captured by the AVM Act set a considerably high threshold for IHCSP, government and law enforcement action to remove online material, balancing the protections of the Act with freedom of speech and public interest tests.

The AVM Act

The Act established, for the eSafety Commissioner, a power to issue a notice stating that, at the time the notice is issued, a content or hosting service was providing access to, or hosting, AVM in contravention of Australian law. Whilst a notice issued by the eSafety Commissioner does not mean an offence has been committed, it creates a rebuttable presumption in relation to a future prosecution that the provider was reckless as to whether AVM was hosted on their service.

In support of the AVM Notice, the legislation established two new offences:

- **Failure to Report**—an offence for IHCSPs that fail to notify the AFP within a reasonable time about material relating to abhorrent violent conduct occurring in Australia.
- **Failure to Remove**—offences for content service and hosting services that fail to remove access to abhorrent violent material expeditiously where that material is reasonably capable of being accessed within Australia.

These offences are intended to ensure that IHCSPs take responsibility for referring to the AFP and removing AVM that can be accessed using, or on, their services thereby reducing the impact and reach of AVM sought by perpetrators who intend to spread their violent and extreme propaganda. There are defences built into each offence, including, critically, to ensure that content and hosting services are not liable for failing to remove AVM where maintaining access to that material is necessary for law enforcement purposes.

As at 20 September 2021, the Department understands that:

- The eSafety Commissioner has investigated more than 2,049 reports about AVM since the legislation came into effect in April 2019.
  - The vast majority of these reports (over 98 per cent) related to child sexual abuse material. Generally, the eSafety Commissioner refers child sexual abuse material to the relevant INHOPE member country for rapid takedown, or notifies the AFP, rather than issuing an AVM notice.
- The eSafety Commissioner has issued 24 AVM notices against 15 items of content.
  - As a result of these notices, 13 out of 15 items of content (87 per cent) were either taken down or restricted for Australian end-users.
- There have not been any prosecutions, and consequently no pecuniary (or custodial) penalties have been imposed.

The AVM Act is not designed as an instrument of pure prosecution; the provisions of the legislation mean that the Act also serves as a deterrent mechanism to discourage inaction by IHCSPs in relation to AVM online. As the eSafety Commissioner has only issued 24 AVM notices against 15 items of content in the last two years, data is reasonably limited. The available data, set out above, suggests that the AVM notification scheme has had a positive deterrent effect to date, with 87 per cent of items of content being taken down or restricted for Australian end-users following the receipt of an AVM notice by a content or hosting service.

Significantly, nearly all AVM notices (bar one) have been issued to content service providers and hosting providers based offshore. This suggests that Australia's current regulatory framework is making it increasingly undesirable to host AVM online in Australia.

Though the Act is just two years old, and there will continue to be a need to assess the efficacy of the Act over the coming years, it is clear from the aforementioned statistics that the large majority of AVM cases are effectively dealt with under the Act's notice provisions. Through this lens, the Department considers that the AVM Act is effective.

Challenges and Opportunities

There is opportunity to consider whether referral and investigation processes can be further streamlined and clarified. Going forward, we will continue to work across Government to ensure that the AVM Act is working effectively operationally.

Though extraterritoriality has not hindered the AVM Act to date, and the circumstances to test the offences have not arisen, it is reasonable to expect that the AVM Act's ability to ensure that IHCSPs take timely action to remove or cease hosting AVM on their platforms may face future challenges where those IHCSPs are not located in Australia. Any such challenge may be further exacerbated by encrypted networking and new hosting arrangements, which make it more difficult to determine where content is hosted.

At present, there are no formal mechanisms to enforce extraterritorial notices from the eSafety Commissioner for AVM content to be removed. The Global Internet Forum for Counter Terrorism (GIFCT) is a not-for-profit organisation which brings together the technology industry, government, civil society and academia, to foster collaboration and information sharing to counter terrorist and violent extremist activity online. It is funded by, and its Operating Board comprises of, Microsoft, Twitter, Google and Facebook. A key element of the GIFCT's remit is to build the capacity of smaller platforms to respond to terrorist content on their service and in future, there may be options to leverage these relationships to have AVM content removed. The GIFCT offers two cross-platform programs (available only to members) – a hash sharing database and a URL sharing regime – to prevent member services from being a conduit for AVM content. Currently, the GIFCT is a mechanism for governments to engage with predominately United States-based Big Tech companies; however it does not represent the platforms on which AVM is more likely to be hosted.

Ongoing collaboration between governments and industry, including in multilateral fora, to better link Australia's domestic efforts to counter online harms with emerging and deepening international norms, will be critical in addressing these challenges.