Contents

Foreword vii
Acknowledgements ix
Abbreviations xi
Contributors xiii

1. Rethinking social media and extremism 1
   Shirley Leitch and Paul Pickering

2. The making of a ‘made for social media’ massacre 13
   Shirley Leitch

3. Becoming civic actors 43
   Sally Wheeler

4. Hate the player, not the game: Why did the Christchurch shooter’s video look like a game? 65
   Robert Fleet

5. Brand lone wolf: The importance of brand narrative in creating extremists 87
   Andrew Hughes

6. ‘Clumsy and flawed in many respects’: Australia’s abhorrent violent material legislation 103
   Mark Nolan and Dominique Dalla-Pozza

7. Coarse and effect: Normalised anger online as an essential precondition to violence 125
   Mark Kenny

8. Performances of power – the site of public debate 143
   Katrina Grant

9. Crisis, what crisis? 159
   Terhi Nurmikko-Fuller and Paul Pickering
‘Clumsy and flawed in many respects’: Australia’s abhorrent violent material legislation

Mark Nolan and Dominique Dalla-Pozza

Introduction

An alarming feature of the Christchurch mosque attacks was the fact that the perpetrator went not only armed, but also rigged up with a camera to fulfil his plan of livestreaming the attacks on the internet. In addition to the writing of a manifesto and the detailed planning of the attack itself, the attacker successfully fulfilled his intention of broadcasting the attack on the internet. As described by Douek (2020, p. 41):

---

1 This chapter was initially developed and presented for the symposium ‘After Christchurch: Violent Extremism Online’ hosted by the ANU Australian Studies Institute and held at the ANU College of Law, Canberra, on 29 August 2019. A form of this paper was presented at the Joint Conference of the Australian and New Zealand Association of Psychiatry, Psychology and Law and the Forensic Faculty of the Royal Australian and New Zealand College of Psychiatry, Collaboration and Challenges Across the Global South, held in Singapore on 5–8 November 2019. The authors also made a submission (submission 15) to the Parliamentary Joint Committee on Law Enforcement inquiry on the Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019 in November 2021, which drew upon the material in this chapter. See www.aph.gov.au/Parliamentary_Business/Committees/Joint/Law_Enforcement/AVMAct/Submissions.
When the shooter entered the Christchurch mosques on Friday 15 March 2019, he was armed not only with guns but also with a helmet camera that streamed the attack live on Facebook. For the next 16 minutes and 55 seconds, the footage of his horrific violence was broadcast around the world in real time on Facebook Live.

In the aftermath of this broadcast the Australian Government acted swiftly and exceptionally to pass the *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019* (Cth) in an attempt to reduce the risk of broadcasting such terrorist attacks in the future. In this chapter we are critical of the way in which this legislative desire was achieved, arguably in pursuit of a very noble aim to avoid the additional suffering that was caused by the broadcast of such horrendous attacks.

Our criticisms centre firstly around the unusual features of the legislative process used at this time, in the lead-up to an election, particularly the lack of parliamentary debate and the absence of committee consideration; and, secondly, the nature of the regulatory regime created, implicating an arguably under-resourced and under-prepared eSafety commissioner, and its links to problematic offence definition. There are some controversial ways of establishing the fault elements in some of the new offences created. These concerns resonate with the surprised reactions of some other commentators (e.g. Douek, 2020) who, like us, worry about the potentially negative consequences of yet another piece of hastily drafted and powerful counterterrorism law affecting both telecommunications and internet companies and individuals alike.

**Process problems with the passage of the *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019* (Cth)**

**Little substantive parliamentary debate**

An analysis of the parliamentary debate of the *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019* (the AVM Act) reveals a number of striking features. The first is that the legislation was explicitly framed as a direct response to the shootings in Christchurch. Attorney-General Christian Porter opened substantive debate on the Bill ‘by paying tribute to all those who suffered and lost their lives and lost
loved ones as a result of the Christchurch terrorist attack’ (Commonwealth, 2019a, p. 1849). He then moved to argue that the AVM Bill was required to address two infamous features of the Christchurch attack: the livestreaming of the shooting on social media and the fact that that recording was available for viewing or download on those platforms for over an hour (Commonwealth, 2019a, p. 1849; Douek, 2020, p. 45). As the attorney-general said, ‘we must act to ensure that perpetrators [of terrorist acts] and their accomplices cannot leverage online platforms for the purposes of spreading their violent and extreme … propaganda’ (Commonwealth, 2019a, p. 1849; see also Commonwealth, 2019b, paragraph 2).

A similar structure is observable in the opening comments by non-government parliamentarians who contributed to debate in the House of Representatives. Shadow Attorney-General Mark Dreyfus acknowledged ‘[t]he terrorist atrocity committed in New Zealand’ (Commonwealth, 2019c, p. 1851) and then moved to outlining the Opposition position: ‘Labor believes that social media companies must do more in preventing the dissemination of material produced by terrorists showing off their crimes’ and therefore the Opposition would support the Bill ‘despite reservations’ (Commonwealth, 2019c, p. 1852). The Australian Greens indicated that ‘[w]e all grieve with New Zealand’ (Commonwealth, 2019d, p. 1855) and signalled that their party had previously advocated for more legislative changes in relation to social media (Commonwealth, 2019d, p. 1856). Independent MP Kerryn Phelps directly called the events in Christchurch a ‘catalyst’ for the legislation (Commonwealth, 2019e, p. 1857).

While the explicit linking of the AVM Bill with the events in Christchurch was a noticeable feature of the parliamentary process, it was not an unusual one. It is reasonably common for pieces of Australia’s (now complex) counterterrorism law framework to be developed or adjusted in reaction to various terrorist atrocities (Lynch et al., 2015, pp. 198–200, Blackbourn et al., 2019, pp. 186–87). For example, the terrorist attacks in the US on 11 September 2001 catalysed major Australian counterterrorism law reform as did the London bombings of 2005 (Lynch et al., 2015, p. 198). Indeed, as one of us has written, the experience of counterterrorism law-making since 2001 means it is likely that substantial amendments to Australia’s counterterrorism laws will be made ‘in the shadow of a crisis’ (Dalla-Pozza, 2016, pp. 272, 278). While there are many reasons why legislators should choose to alter legislation in response to events such
as the Christchurch massacre, law-making in such circumstances carries particular challenges (Dalla-Pozza, 2016, p. 282; Lynch et al., 2015, pp. 195–205).

One such challenge is that the time that parliament has to debate these laws can be significantly shortened. The AVM Bill is an especially egregious example of this phenomenon. The Bill was introduced in the Senate on 3 April 2019, mere weeks after the events in Christchurch. As events transpired, 3 April was also the last sitting day when the Senate could consider legislation before the parliament was prorogued prior to the 2019 election (Parliament of Australia, 2019). There was controversy about the 2019 parliamentary sitting calendar with the Labor Opposition claiming that the Morrison Coalition government was seeking to minimise the ability of parliament to provide scrutiny (see Belot, 2018). Some of the background to the 2019 election, including the events that led to the Morrison government lacking an absolute majority in the House of Representatives by early 2019, are usefully summarised by Muller (2020, pp. 3–4). The Senate Hansard for that day records the fact that the events in Christchurch were discussed on this day (see e.g. Commonwealth, 2019f, p. 828). However, there was almost no discussion of the AVM Bill itself. Indeed, while the Hansard indicates that the Bill passed through all the stages formally required, no substantive debate on the Bill is recorded (Commonwealth, 2019f, pp. 992–93). The Bill then moved to the House of Representatives where it was introduced and debated on 4 April. Again, this was the last day that the House had to consider legislation. Just under one hour was spent debating the legislation before it was passed (Commonwealth, 2019g, pp. 1849–60). This only allowed for contributions from four members of parliament: the attorney-general (Christian Porter), the shadow attorney-general (Mark Dreyfus), the leader of the Australian Greens (Adam Bandt) and an independent (Kerryn Phelps). The Bill was given Royal Assent, the final stage required before it became law, on the following day.

It should be recognised that it is impossible to put forward blanket prescriptions of how much time parliament should spend publicly considering legislative proposals. Parliamentary time does need to be used appropriately (Uhr, 1998, pp. 124–25, 219–21; Lynch, 2006, p. 779). The amount of consideration time each piece of legislation receives can be influenced by a number of factors (Dalla-Pozza, 2010, pp. 157–58). However, we would argue that the AVM Act required more sustained parliamentary attention than it received. As Douek observes, ‘writing laws
to create social media reform is hard and involves difficult trade-offs’. She mentions the particular complexity of ensuring that ‘freedom of expression’ is not unduly curtailed by such laws (Douek, 2020, p. 42). However, as will be outlined below, this is only one of the many issues that underpin the AVM Act. Douek (2020) also notes that the Morrison government announced that the AVM Bill was ‘a world first’ (Douek, 2020, p. 42). This suggests that the legislation was novel, as well as being complex. As such, it is difficult to accept that a public law-making process that took place over a mere three-day period (from 3–5 April 2019), and that afforded parliamentarians less than one hour of substantive debate on the features of the Bill, is adequate or appropriate.

**Absence of scrutiny by the Parliamentary Joint Committee on Intelligence and Security (PJCIS)**

Another striking feature of the parliamentary process that produced the AVM Act was the absence of parliamentary committee scrutiny of this legislation. The shadow attorney-general remarked upon the fact that the Bill had not been referred to the PJCIS (Commonwealth, 2019c, p. 1852) and the Greens MP even tried to move an amendment attempting to refer the Bill to that committee, an amendment that was voted down (Commonwealth, 2019d, p. 1856; Commonwealth, 2019f, pp. 1858–60). There is no binding requirement that a piece of law directed to countering terrorism or national security must be referred to this committee. Nevertheless, recent assessments of the work of the PJCIS suggest that it is unusual for a piece of legislation like the AVM Act to be passed without this committee having the opportunity to scrutinise it. In 2018 Moulds commented that since 2013 the PJCIS ‘has inquired into and reported … on each of the key legislative reforms’ that related to counterterrorism and national security law (Moulds, 2018, p. 287). Similarly, in the recently released *Comprehensive Review of the Legal Framework of the National Intelligence Community*, Richardson commented that ‘[i]t is usual practice for Bills relating to national security to be referred’ to that committee (Richardson, 2019, p. 21).

The most obvious explanation for the absence of PJCIS scrutiny of the AVM Bill lies in the fact that there was the clear expectation that the parliament would be prorogued prior to an election within days of the AVM Bill being introduced (Commonwealth, 2019c, pp. 1852, 1854). If the Morrison government had referred the AVM Bill to the PJCIS it
may have delayed the passage of the Bill, and, in these circumstances, probably have ensured that the Bill would not have been passed before the 2019 election. It is also true that the AVM Act contains a provision that mandates some review of the provisions contained within it. The Act itself specified that, two years after these new provisions commenced, ‘the Minister must cause to be conducted a review of the operation’ of the provisions (s. 474.45). This report needed to be given to the minister within a year after it commenced, and the report needed also to be tabled in the parliament. In fact, the Parliamentary Joint Committee on Law Enforcement was tasked by the attorney-general to complete this review. This committee completed its report on the Act in late 2021 (Parliamentary Joint Committee on Law Enforcement, 2021, p. 1). To the best of our knowledge, at the time of writing, there is no public document outlining the government’s response to this review (Parliamentary Joint Committee on Law Enforcement, 2022).

Despite some review process being included, the impact of the absence of expected parliamentary committee scrutiny for this Bill prior to its passage should not be underestimated. One of the key criticisms of the AVM Act that emerges from both the limited parliamentary debate (Commonwealth, 2019e, p. 1858; Commonwealth, 2019c, p. 1854), and from initial academic consideration of the Act, is that in producing the Act ‘[t]he government did not consult with experts, civil society or industry’ (Douek, 2020, p. 42). Definitely, as suggested by Douek, there was no connection or reference to the ongoing work being completed by the Australian Taskforce to Combat Terrorist and Extreme Violent Material Online, which reported only a few months after the Christchurch bombings (Douek, 2020, p. 58).

There are two main problems associated with this lack of consultation. Firstly, as will be further discussed, there were many complex aspects of this Bill. It is possible that if a parliamentary committee such as the PJCIS were allowed to scrutinise the Bill, and call for submissions from non-government entities or scholars, alternative ways of responding to the challenge of using the criminal law to regulate the appearance and spread of abhorrent violent material online could have been devised.

Secondly, in denying the PJCIS an opportunity to consider the AVM Bill before it was enacted, the parliament was not making full use of its ‘deliberative capacities’ (Uhr, 1998, p. 92; Dalla-Pozza, 2016, p. 273). This is significant because ensuring that the parliament functions more
as a deliberative democratic assembly is one way in which to measure whether an appropriate ‘balance’ has been struck between the competing considerations that underpin counterterrorism legislation more generally (Dalla-Pozza, 2016, pp. 274–75).

These deficiencies of the parliamentary process were a key theme of the contributions from non-government MPs, despite the fact that there was still support for the Bill from those outside of the government, perhaps an indication that all politicians had already begun to be in election mode. While the shadow attorney-general was in the difficult position of having to argue that the Opposition would support the rushed passage of the laws (Commonwealth, 2019c, p. 1853), he also maintained that there needed to be ‘proper consultation’ in relation to the Bill, mentioning that the AVM Bill may not only impact the ‘social media sector’ but ‘traditional media’ as well (Commonwealth, 2019c, p. 1854). Greens MP Adam Bandt opined that ‘because … [the Bill] is being rushed through’, the parliament does not:

Know whether or not the bill in fact does the job the Attorney-General tells us it is doing … we do not know whether or not it goes far enough in stopping that kind of hate speech from being broadcast. (Commonwealth, 2019d, p. 1855)

Similarly, independent Kerryn Phelps commented that ‘laws formulated as a knee jerk reaction to a tragic event do not necessarily equate to good legislation and can have myriad unintended consequences’ (Commonwealth, 2019e, p. 1858). She speculated that one such ‘unintended consequence’ was that international IT companies may avoid Australia to ensure that they are not caught by the AVM Act (Commonwealth, 2019e, p. 1858). This relates to the confident assertion of extraterritorial jurisdiction relating to the offences defined in the Bill.

One of the interesting things about these contributions from parliamentarians is that they illuminate the point that there is a connection between the content of a law and the parliamentary process that produced it. Over the last 20 years, a distinct strand of scholarship that focuses on the connection between legislative processes and the content of specific laws has emerged (see e.g. Lynch, 2006, p. 779; Lynch et al., 2015, p. 198; Carne, 2016, p. 5). It seems clear that the AVM Act was the product of a process that was truly ‘clumsy and flawed’ in many respects (see also
Douek, 2020, p. 60). The following section will examine in more detail the content of the Act and some of the exceptional and problematic aspects of the ‘offence’ definition and related regulatory features of the Bill.

Problems related to the offences created by the Act

In support of and in addition to the important concerns listed by Douek (2020), relating to offence definition or otherwise, we would like to highlight the following matters relating to the content of the Act. This Act is a controversial gap-filling exercise alongside existing cybercrime laws that impose liability for the terrorist offender for also posting material online; that there may not be a high threshold for material to meet the definition of abhorrent violent material; and that there is a tension between proof of subjective fault offences and liability proved via objective fact only, that should concern defence lawyers engaged by providers. First, a brief overview of what offences and defences are created by the AVM Act is in order. We can also note here statements about liability and exposure to notification and prosecutorial powers that have been made publicly by the eSafety commissioner herself. Here, she speaks of the potential impact of the new powers thrust upon her at very short notice, requiring much work by her office, following passage of this Bill in April 2019. Some of her other statements update us about how those new powers have been exercised to date.

The new provisions

Definitions

The definitions provided in the AVM Act are detailed and are of crucial importance to evaluating the potential impact of the new offences created. To begin with, but also avoiding in-depth discussion that these complex definitional provisions deserve, we note that relevant definitions can now be found in s. 474.30 of the Criminal Code (Cth), defining, via an exhaustive ‘means’ definition, that a ‘content service’ is a ‘social media service’ (within the meaning of the Enhancing Online Safety Act 2015 (Cth)) or a ‘designated internet service’ (within the meaning of the Enhancing Online Safety Act 2015 (Cth)). Similarly, a ‘hosting service’ has the same meaning as in the Enhancing Online Safety Act 2015 (Cth) but excludes subparagraphs 9C(a)(ii) and (b)(ii) of that Act.
Importantly, the focus of the *AVM Act* is clearly on the blameworthiness of those *content service providers* and *hosting service providers*, and, clearly, not *internet service providers* (ISPs) or ‘providers of relevant electronic services such as chat and instant messaging services’ as noted in paragraph [8] of the Explanatory Memorandum to the Bill (Commonwealth, 2019b, p. 6).

The Act provides definitions for ‘abhorrent violent conduct’ (AVC) and ‘abhorrent violent material’ (AVM) in the new Subdivision H (‘Offences relating to the use of carriage service for the sharing of abhorrent violent material’) of Division 474 (‘Communications Offences’) in the *Criminal Code* (Cth). The latter relies on the former for its meaning.

The definition of AVM, now found in s. 474.31 of the *Criminal Code* (Cth), states the following, via another exhaustive ‘means’ definition:

**474.31 Abhorrent violent material**

1. For the purposes of this Subdivision, *abhorrent violent material* means material that:
   a. is:
      i. audio material; or
      ii. visual material; or
      iii. audio-visual material;
      that records or streams abhorrent violent conduct engaged in by one or more persons; and
   b. is material that reasonable persons would regard as being, in all the circumstances, offensive; and
   c. is produced by a person who is, or by 2 or more persons each of whom is:
      i. a person who engaged in the abhorrent violent conduct; or
      ii. a person who conspired to engage in the abhorrent violent conduct; or
      iii. a person who aided, abetted, counselled or procured, or was in any way knowingly concerned in, the abhorrent violent conduct; or
      iv. a person who attempted to engage in the abhorrent violent conduct.
2. For the purposes of this section, it is immaterial whether the material has been altered.

3. For the purposes of this section, it is immaterial whether the abhorrent violent conduct was engaged in within or outside Australia.

It is worth noting here that what makes the material ‘abhorrent’, it seems, is the definitional element in s. 474.31(1)(b), namely, that the audio material, visual material or audio-visual material that records or streams abhorrent violent conduct engaged in by one or more persons (s. 474.31(1)(a)), and is material that reasonable persons would regard as being, in all the circumstances, offensive. This objective reasonable-person test, qualified by noting the contextual circumstances, resonates with the objective tests for cyber offensiveness that has been used in relation to the pre-existing s. 474.17 Criminal Code (Cth) offence of using a carriage service to menace, harass or cause offence (see below).

The definition of AVC, now found in s. 474.32 of the Criminal Code (Cth), is notably much broader than merely including terrorist act offences, defined to be the same as in s. 100.1 of the Criminal Code (Cth) excluding paragraphs 100.1(2)(b), (d), (e) and (f). Interestingly, the AVM Act includes a much broader range of offences in its definition of AVC, so, it was a net-widening opportunity to respond to more than the features of the Christchurch attack livestreaming alone:

**474.32 Abhorrent violent conduct**

1. For the purposes of this Subdivision, a person engages in abhorrent violent conduct if the person:
   a. engages in a terrorist act; or
   b. murders another person; or
   c. attempts to murder another person; or
   d. tortures another person; or
   e. rapes another person; or
   f. kidnaps another person.

In order to work with all elements of these definitions, and offence types further defined within the AVM Act, a rather detailed knowledge of some of the most complex criminal offences defined in the Criminal Code (Cth), or elsewhere, is required. This places an enormous burden upon not only staff in the Office of the eSafety Commissioner, but also upon the lawyers or others within companies, community organisations
or other groups and upon any individuals providing content and hosting services. Anyone assessing the content of internet postings must possess an understanding of whether the material in question represents criminal liability, not only for terrorism, which would be challenging enough to assess, but also for four other types of criminal offence, including what it means to attempt murder.

**Offences**

Two new offences are created by the *AVM Act*.

**The failure to notify offence**

The first offence defined under s. 474.33 of the *Criminal Code* (Cth) is a failure to notify offence, placed upon a provider located anywhere in the world (a form of extraterritoriality that again involves a broad investigative and regulatory scope with extensive resource implications). It criminalises awareness that the AVM can be accessed by a service that the defendant manages when they have reasonable grounds to believe that the AVM material is recording or streaming AVC that has or is occurring in Australia (at least that requirement is some form of geographical limit here), and when the defendant individual or organisation/company does not refer the existence of that AVM to Australian Federal Police (AFP) within a ‘reasonable time’. A similar failure to notify offence already existed in the *Criminal Code* (Cth) under s. 474.25 in relation to child pornography and child abuse material on the internet, albeit with considerably less serious maximum penalties.

Crucially, no further definition of ‘reasonable time’ is given. There is some further detail about this provided in the Explanatory Memorandum but there will still be a need for parties to any prosecution to debate what ‘reasonable time means’ when that is applied to the specific facts of failure to notify behaviour:

A ‘reasonable time’ is not defined. A number of factors and circumstances could indicate whether a person had referred details of abhorrent violent material within a reasonable time after becoming aware of the existence of the material. For example, the *type and volume of the material*, and the *capabilities of and resourcing available to the provider may be relevant factors*. In a prosecution for an offence against section 474.33, the determination of whether
material was referred within a reasonable time will be a matter for the trier of fact. (Commonwealth, 2019b, p. 19, paragraph [39], emphasis added)

It is encouraging here, in the interests of potential defendants, that resourcing available to the provider is listed as a potential reason to shape the definition of ‘reasonable time’, perhaps allowing that time to be defined as longer than may otherwise be the case for better-resourced providers.

This offence carries a maximum penalty of a fine of $168,000 for natural persons and a fine of $840,000 for corporations (Commonwealth, 2019b, p. 19, paragraph [40]). As with some similar decisions to charge individuals and corporations, including those based overseas, with Criminal Code (Cth) offences, the attorney-general needs to give written consent before ‘proceedings’ can begin under s. 474.33 if the conduct that is alleged to constitute an offence under the section occurs entirely overseas and the individual charged is not an Australian citizen or the corporation involved is not incorporated under Australian law (under 47442(1)) but arrests can be made prior to that consent to charge being given (s. 474.42(2)) (see also Douek, 2020, pp. 43).

The failure to remove offence

The second offence created under s. 474.34 of the Criminal Code (Cth) criminalises the failure of relevant providers based anywhere in the world to effect ‘expeditious removal’ of AVM able to be accessed within Australia. Subjective fault elements of recklessness are provided by the drafters of this offence as attaching to the physical elements of whether the material is AVM and whether the material can be accessed within Australia. The usual relevant federal criminal law definition of subjective recklessness under s 5.4 of the Criminal Code (Cth) that would normally apply here for individuals would be:

5.4 (1) A person is reckless with respect to a circumstance if:

a. he or she is aware of a substantial risk that the circumstance exists or will exist; and

b. having regard to the circumstances known to him or her, it is unjustifiable to take the risk.
For corporations, the detailed provisions set out in Part 2.5 of the *Criminal Code* (Cth) would normally apply, allowing recklessness of a corporation to be proved more indirectly from a range of organisational dynamics including corporate culture (Clough, 2007; Clough, 2017; Clough and Mulhern, 2002).

The removal expected would render it inaccessible to end users of the service (s. 474.34(15)). Again, the crucial temporal element of ‘expeditious’ was not defined in the *AVM Act* (see also Douek, 2020, pp. 45–46, 49) but there is speculation within the Explanatory Memorandum that may assist interpretation of that physical element of the offence when it comes the time for that debate to be had at trial:

[51] ‘Expeditious’ is not defined and would be determined by the trier of fact taking account of all of the circumstances in each case. A number of factors and circumstances could indicate whether a person had ensured the expeditious removal of the material. For example, the type and volume of the abhorrent violent material, or the capabilities of and resourcing available to the provider may be relevant factors. (Commonwealth, 2019b, p. 19, paragraph [51], emphasis added)

It is again reassuring that there will need to be a debate between parties to a prosecution about the relevant definition of ‘expeditious’ that would apply to a particular case, though the lack of definition here again speaks to a gap left by absent scrutiny of and consultation on one of the more important aspects of the offence definition before passage of the legislation. These are matters that we would normally expect quite rigorous debate upon during a parliamentary debate of greater length.

The penalties for this offence are more severe than for the failure to notify offence, with individuals being liable to a maximum penalty of three years imprisonment or around a $2.1 million fine or both, corporations being liable for the greater of around $10.5 million or 10 per cent of their annual turnover during the 12-month period up to the end of the month within which the offence occurred (s. 474.34). Interestingly, the attorney-general’s written consent is needed for charging (s. 474. 42(3)) penalties, but arrests may occur before that consent is given (s. 474.42(4)).
Defences

Defences provided by the *AVM Act* in ss. 474.37–474.38 to the offence provisions cover a range of people including journalists, law enforcement agencies, public officials, researchers, political advocates (protected by a recitation of the implied constitutional freedom of political communication) or artists who may have copied the AVM before it was taken down. These are important protections for a range of people needing to access and share AVM portraying regulated AVC (but see the concerns raised by Douek, 2020, pp. 53, 57).

What the *AVM Act* adds to existing cybercrime laws

It is useful to note from the outset that the *AVM Act* did not provide any new powers or any new creative regulatory ideas about preventing or prosecuting terrorists who plan to livestream their attacks on the internet or otherwise publish AVM on the internet. The attorney-general explained in his Explanatory Memorandum to the Bill that the intention of the drafters of the Bill was to:

> Address significant gaps in Australia’s current criminal laws by ensuring that persons who are internet service providers, or who provide content or hosting services, take timely action in relation to abhorrent violent material that can be accessed using their services. This will ensure that online platforms cannot be exploited and weaponised by perpetrators of violence. (Commonwealth, 2019b, para [2])

To clarify, the new provisions do not attempt to regulate the sharing of abhorrent violent material (AVM) via new and targeted cybercrimes that criminalise the specific posting of AVM by a lone actor terrorist or any other person or terrorist group. That potential liability seems already covered by the intersecting web of federal cybercrime offences that had existed for considerable time pre-Christchurch. Such cybercrime laws, for example, include the s. 474.17 offence of using a carriage service to menace, harass or cause offence (where offensiveness is what the reasonable person in all the circumstances would consider offensive as provided by s. 474.17(1)b; see *Crowther v Sala* [2007] QCA 133 for an in-depth discussion of the offensiveness test and other elements of that offence; and *Waterstone v R* [2020] NSWCCA 117 for a recent application of such a test). Furthermore, the s. 474.15 offence of using a carriage service to make a threat, and the s. 474.14 offence of using a telecommunications
network with intention to commit a serious offence, for example, any federal terrorism act or terrorist organisation, or preparation of terrorism offence (or other AVC), could be used against the person who livestreams or posts the AVM to the internet in the first instance.

**Attempted reassurance given by the eSafety commissioner**

The eSafety commissioner notes in her factsheet (eSafety Commissioner, 2020) that the federal government held a meeting after the Christchurch attacks with digital services and ISPs regarding AVM, and with industry stakeholders after the legislation was passed to workshop the process for sending and receiving notices, and with ‘smaller and mid-tier platforms hosted overseas to establish contacts and escalation paths and advise a broader range of companies about the AVM scheme’ (eSafety Commissioner, 2020). Helpfully, the commissioner suggests in her factsheet that ahead of issuing an AVM notice, informal contact can be made with services to notify them unofficially that material is likely to violate that platform’s own community standards.

Beyond this attempt to show preparedness by the eSafety commissioner to walk with stakeholders during this regulatory journey, the point can be made that even this level of consultation, engaged in following the passage of the legislation as well as after the attacks and before the parliamentary ‘debate’, is limited and only goes so far, as Douek (2020) argues. This level of consultation may not have engaged with many smaller scale or currently unknown content service providers and hosting service providers without profile in the industry and without strong and ongoing existing relationships with the commissioner.

In this sense, this level of consultation may have come far too late and may have only reached a small fraction of affected persons, companies and groups. It may contextualise only a small subset of those potentially affected by the possible exercise of the eSafety commissioner’s discretion. Even these attempts may mean that many smaller providers could remain under-educated, potentially unknown to the eSafety commissioner, and exposed more easily to damaging potential liability under this new regime. Monitoring the exercise of discretion by the eSafety commissioner and the Commonwealth director of public prosecutions is integral to revealing
if there is overreach of these new provisions in prosecutions against smaller providers. A review of the Annual Report of the Commonwealth Director of Public Prosecutions and case analysis over time will reveal if the prosecution rates against content and hosting service providers are problematic.

The eSafety commissioner’s factsheet published on 24 March 2020 notes further that there were, up to that time, 18 notices issued to:

10 worst-of-the-worst underground gore sites and services that host these sites. The material showed beheadings, shootings and other murders. The notices prompted the removal of 70 per cent of this material. (eSafety Commissioner, 2020)

In that factsheet, apparently aimed at appeasing concerned content and hosting service providers, the eSafety commissioner attempts to reassure all that her powers will only be used ‘in the most extreme cases … [and that the commissioner] does not monitor the internet for AVM and it is predominantly a complaints-based regime’ (eSafety Commissioner, 2020). The fact that there are no resources to attempt the style of systematic monitoring of the internet that seems assumed by the powers given by the AVM Act is of no particular reassurance to those who will become potentially liable under it. In the same factsheet, the commissioner suggests that she: ‘assesses material on a case-by-case basis, using discretion to determine whether it is appropriate to issue a notice. This is not a heavy-handed approach’ (eSafety Commissioner, 2020). Despite those attempts to reassure all that the commissioner is reluctant to use her considerable new powers, some worries obviously remain.

The threshold for the material to meet the definition of ‘abhorrent violent material’

The eSafety commissioner has suggested that there is a ‘very high threshold for material to meet the definition of AVM’ (eSafety Commissioner, 2020). To agree with this statement would be to fail to acknowledge that, at least for terrorist act offences under the Criminal Code (Cth), the behavioural threshold for liability is not always set at a high level. Highly preparatory terrorist act offences exist in the Code, and, together with the definition of that form of AVC with the definition of the AVM, it could be said that the threshold for some recorded or streamed behaviour to satisfy the tests for AVM/AVC could likely be quite lower than asserted. Even the
restrictions on who needs to produce the AVM under s. 474.31(1)(c), as set out above, could be thought to include such a significant number of potential persons that the threshold for defining online content as AVM should not be considered particularly high.

Proof of fault elements via responses to notices issued by the eSafety commissioner

Perhaps those at most risk of prosecution are not the corporations and major stakeholders with existing relationships of trust and consultation with the eSafety commissioner, but those small organisations and individuals who are suspected more easily of acting in bad faith. For those most vulnerable potential defendants of the failure to notify or remove offences, most troubling is how the required full subjective fault offences may be proved beyond reasonable doubt. Especially concerning is a twist on the required fault element proof that exists for the failure to remove offence in particular. As a result of s. 474.34(5), recklessness can be presumed merely by the objective facts that the eSafety commission has issued a notice about AVM (that a provider may not have received or understood) and that the access to the AVM can still be made following issuance of that notice. Subjective recklessness can therefore be proved by those objective facts alone rather than being proved beyond reasonable doubt on the standard subjective fault element tests as referred to above.

The eSafety commissioner’s factsheet on these provisions supports our opinion that a controversial, evidentiary shortcut to proof of a subjective fault element exists and that there is some legal benefit in the commissioner issuing an AVM notice. Having issued a notice, recklessness as to failing to take down the material can be proved, not by examining the subjective mind of the individual or corporation who failed to remove or cease hosting AVM as per s 5.4 (1) or Part 2.5 of the Criminal Code (Cth), but merely as a presumption associated with the objective facts that the identified material has not been removed following the issuing of a notice:

This [the issuing of a notice] is not a power to take down material. The notices do not require the AVM to be removed. However, if a service is later prosecuted for failing to remove or cease hosting AVM, the notice can be used in legal proceedings to show recklessness regarding the AVM. (eSafety Commissioner, 2020)
The ability to prove recklessness in this way seems to suggest that the drafters really wanted this offence to contain strict or absolute liability elements; however, the more controversial presumption mechanism was used to dilute the otherwise apparent requirements to prove full subjective fault. If there was a greater level of debate in parliament or in committee or via public consultation about these aspects of offence definition we wonder if it would have drawn more controversy.

**Conclusion**

The provisions introduced by the post-Christchurch Bill aimed at regulating the sharing of abhorrent violent material can be considered ‘clumsy and flawed in many respects’ and at least in two senses. Firstly, the hasty introduction of the Bill and its extremely short and under-deliberated passage through parliament suggests that there was limited time devoted to publicly debating these provisions.

This is particularly concerning when the nature and breadth of the powers and offences created by the Act are examined, despite reassurances from the eSafety commissioner herself. The way in which full subjective criminal liability is created by the Act, and fault elements of recklessness in the failure to remove offence in particular, can be proved via objective facts alone, and may mean that it is easy for some content service or hosting service providers to fall foul of the new offences, perhaps, especially if those providers are individuals or not large, well-known and informed corporations providing content or hosting services. In that and other contexts, these offences are controversial, and their extraterritorial reach and potential impact on international relations, if not international commerce, seemed to have warranted much more parliamentary debate than was afforded at the time (see also the discussion in Douek, 2020 p. 58).

The work of the eSafety commissioner as well as the discretion that may be exercised in favour of content service or hosting service providers by the Commonwealth director of public prosecutions will be interesting to monitor into the future. Any imbalance between a focus on prosecuting large, well-known corporations versus individuals under this new regime will be important to analyse, as will the relative use of failure to remove offences versus failure to notify offences. The financial and technical assistance required for some providers to even detect, if not also be able to remove, material that satisfies the complex legal definitions of AVM is
something that the eSafety commissioner and the government of the day should consider. Any unintended consequences will be lamentable, and perhaps could have been preventable, in light of the haste and exceptionally thin deliberative processes used to pass such powerful provisions.

References


6. ‘CLUMSY AND FLA WED IN MANY RESPECTS’


