Group submission to the Parliamentary Joint Committee on Law Enforcement

in relation to the AVM Act

Committee Secretary
Parliamentary Joint Committee on Law Enforcement
PO Box 6100
Parliament House
Canberra ACT 2600

By email: le.committee@aph.gov.au

Dear Sir/Madam,

We thank you for the opportunity to respond to the Inquiry into the *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019* (AVM Act).

This submission is made on behalf of a group of local and global technology companies, industry and business associations, civil society and academics to express **shared concerns around implementation challenges and unintended consequences of the AVM Act.**

As a group, we wholeheartedly support the intent of the AVM Act and are committed to working with the Australian Government to give effect to the law in a way that ensures those individuals and corporations who deliberately or wilfully distribute or host Abhorrent Violent Material are the subject of strong penalties.

We came together informally in 2019 to share information about obligations and unintended consequences under the Act, after it was passed with urgency in the aftermath of the Christchurch terror attacks.

At the time we were given a Fact Sheet from the Attorney-General's Department to help industry understand the purpose and intentions of the AVM Act. However, it was our concern that the obligations contained within the AVM Act were much broader than was intended and outlined by the Attorney-General's Department, and that this would have unintended consequences.

We developed a **summary of our key concerns along with some proposed solutions** in the form of draft amendments. We provided this to the Government in September 2019 and have attached it to this letter as the bulk of this submission. These concerns relate to the effectiveness and appropriateness of provisions within the AVM Act (i.e., Inquiry Terms of Reference A, B, C and D).

Please note that whilst the Department's updated AVM Fact Sheet[1] is useful, the issues outlined in our summary proposal remain of concern to us.

We hope that by sharing our concerns we can encourage support for updating the AVM Act to align more closely with the guidance provided by the Department. This would provide clearer guidance for industry and stakeholders, all the while maintaining the intent and effectiveness of the AVM Act.

---

[1] https://www.ag.gov.au/crime/publications/abhorrent-violent-material-act-fact-sheet.

This submission includes:

- Our summary proposal that was shared with the Government in 2019, including our key concerns, suggested amendments and five practical case studies.

Sincerely,

Communications Alliance

Digital Industry Group Inc.

Digital Rights Watch

Tik Tok Australia and New Zealand

Google Australia and New Zealand

IBM Australia

Twitter Australia and New Zealand

Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019
Summary of concerns, suggested amendments and supporting case studies

1. Background

As you are aware, the *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019* **("the Act")** commenced into law on April 5, 2019, as part of the Australian Government's approach to combat violent extremist and terrorist content online in the aftermath of the tragic Christchurch terrorist attacks in March. In the lead up to the last election, the Act passed within 48 hours of its introduction to the Parliament, without consultation with industry.

Terrorism and violent extremism are complex societal problems that require an all-of-society response. As a group that represents the interests of local and global technology companies, industry and business associations, civil society and academics, we wholeheartedly support the intent of the Act and are committed to working with the Australian Government to give effect to the law in a way that ensures those who deliberately or wilfully distribute or host Abhorrent Violent Material (AVM) are the subject of strong penalties. AVM can be video footage but also includes still images such as photos and audio material.

The purpose of this document is to set out our proposed concerns, suggested amendments to the Act and supporting case studies. We are grateful to the government for inviting us to provide this information and the Prime Minister's recent statement about working with industry on this issue.

We believe some minor amendments to the legislation - which alter wording within some provisions but do not change the intention of the Act - will provide clearer guidance for industry and stakeholders while maintaining the intent and effectiveness of the Act.

2. Summary of key concerns

Our concerns are listed below in order of priority (starting with the highest priority). The accompanying proposed amendment is referenced and outlined in the table in the next section of this document **[3].**

CORE AREAS

1. **Awareness and action.** For many organisations the monitoring obligations triggered by the Act are unclear. i.e. Guidance has been given by the Department of the Attorney-General that there is no obligation to proactively monitor but the Act can be interpreted to confer monitoring obligations on providers. This is because the Act presumes providers to be reckless at the time that a notice is issued by the eSafety Commissioner in combination with the associated definition of recklessness. (Note that the fault element of recklessness applies irrespective of whether a provider has acted expeditiously to remove AVM). This creates several concerns (addressed in A-C below) which we feel could be remedied through tweaking of the drafting, without distracting

from the intention of the Act, to deem those providers reckless who were aware of the AVM but failed to act expeditiously. We believe these changes will make obligations clearer for small, medium and large businesses, their employees, and nonprofit organisations such as universities and museums (all potential content servers under the act, herein 'providers') [**Amendment A-C].**

2. **Scope includes closed private platforms**. The scope of services caught by the Act is broad and captures business-to-business (B2B) infrastructure and cloud providers. These platforms are private and closed by default rather than open and public facing platforms and are therefore a much lower risk for the widespread dissemination of AVM. For example, large internal IT systems for government departments, airports and banks are highly unlikely to ever contain AVM. Furthermore, B2B infrastructure and cloud providers who host these systems do not and cannot control uploaded content like most public-facing hosts and are usually contractually precluded from reviewing or monitoring content. We ask that the government consider making minor amendments to provide greater certainty for B2B cloud and infrastructure providers **[Amendment D].**

3. **Defences need clarification.** The way in which the AVM Act intersects with art, matters of public interest and political expression online is currently unclear. One interpretation is that the ability to host important historical footage, such as the events surrounding the Holocaust, would be unlawful. We are concerned that uncertainty around these exemptions will lead to the take-down of material not intended to be removed under the Act. We believe some refinements to the defences would help reduce unintended take-down of important and non harmful material **[Amendments E-I].**

4. **No formal review process for the eSafety Commissioner notice**. We appreciate that for a notice to work effectively, it is important the eSafety Commissioner can act quickly. The Department of the Attorney General has advised this was one reason for excluding procedural fairness requirements. The eSafety Commissioner's assessment of content will be subjective and may not consider whether any defences apply to make potential AVM content permissible under the Act. We believe there is a need for a clear process to review any errors made in the issuing of notices. This will give providers certainty and help ensure they are only removing genuine AVM content **[Amendment J]**.

ADDITIONAL AREAS FOR CONSIDERATION

5. **Censorship as a result of over compliance.** Nervousness about the heavy penalties (potential imprisonment or a fine of 10% global revenue) may result in providers erring on the side of caution with removal of content they are unsure about. Some content will clearly be identifiable as AVM but other content may not be, for example where a defence might apply or where it is unclear who produced the content, as the definition of AVM includes that the AVM must be produced by the perpetrator or accomplice - something that is likely to be hard to discern from the footage which can also include still images. An amendment that provides a way for providers to seek information from the e-Safety Commissioner on whether content in the eSafety Commissioner's view actually constitutes AVM will again help to limit unnecessary content removal. It will also help providers operationalise the legislation **[Amendment K].**

6. **Limited transparency around removal of content.** Whenever the Government mandates that public access to information be restricted, it is important to promote transparency so the public understands what has been removed. We believe providers should have the option of explaining to the public why the information is not available. **[Amendment L].**

7. **Disproportionate penalties.** The penalties that apply are out of alignment with other penalties that apply in our legal system. We believe that the most significant penalties be reserved for bad faith actors and/or those who repeatedly and/or flagrantly breach the Act **[Amendment M].**

8. **Difficulty in identifying a 'threat' of kidnapping.** In s474.32 of the Act, kidnapping under *threat* of violence is included as abhorrent violent conduct. This inclusion is not necessary to prevent dissemination of violent material.The lack of actual violence makes implementation of policies to detect and remove AVM more complex for providers. Arguably, the significant penalties imposed by the Act are not appropriate when providers are required to make highly subjective and unreliable decisions about the content **[Amendment N].**

9. **Hard to apply in practice.** The obligation to notify the Australian Federal Police of an offence happening in Australia has an unreasonably low threshold that will be hard to apply in practice. Instead, we would like to work with the government on a practical and meaningful reporting obligation to help ensure the perpetrators of AVM are able to be penalised using the full weight of the law **[Amendment O].**

3. Summary of proposed amendments

For the reasons set out above, we believe the law should be referred to a Parliamentary Committee for review as committed to by the then Minister, Senator the Hon Mitch Fifield on April 4, 2019, who said, “as a matter of good practice, we will, after the election, commission the Senate Communications Committee to inquire into this area of law.”

However, should the government no longer support a referral to a Parliamentary Committee, we believe a small number of minor amendments to the Act would strengthen its effectiveness, provide greater transparency and clarity for providers and users, and preserve the overall intention of the Act. We believe there is scope for these amendments to be passed with support from across the Parliament. These are summarised below.

	CONCERN	**SUGGESTION**	**PROPOSED AMENDMENT**
Awareness and action [concern 1].			
A	The definition of recklessness referenced in the Act is (simplified): A person is reckless in relation to a result/circumstance if (a) the person is aware of a substantial risk that the result/circumstanc e will happen; and (b) having regard to the circumstances known to the person, it is unjustifiable to take the risk. Arguably, almost any provider would need to assume that there is a ‘substantial risk’ that their services could be used for the dissemination of AVM. Whether or not it is unjustifiable to take this risk is subjective and creates unnecessary uncertainty for providers. As currently	A minor amendment to s474.34 will help to remove doubt while maintaining its efficacy. We suggest a tweak in language to clarify there is no requirement for proactive monitoring, so that the obligations are consistent with guidance from the Department of the Attorney-General. This could be done by tweaking sections 474.34(4) and section 474.34(8) so a person shall not be taken to be reckless where they were *not aware* of the AVM on their service.	*Add to section 474.34(4) so that it reads as follows (new words underlined):* “(4) The fault element for paragraphs [...] is recklessness <u>but a person shall not be taken to be reckless in circumstances where the person is not aware of the existence or availability of the specific abhorrent violent material on the content service provided by the person."</u> *Add to section 474.34(8) so that it reads as follows (new words underlined)* "(8) The fault element for paragraphs [...] is recklessness <u>but a person shall not be taken to be reckless in circumstances where the person is not aware of the existence or availability of the specific abhorrent violent material on the hosting service provided by the person.</u> <u>This provision does not require content service / hosting services to proactively monitor the content service / hosting service</u>.”

	drafted, the only way to remove this uncertainty would be to proactively monitor the content on a provider's service which is not the stated intention of the Act.		
B	As we understand it, the stated aim of the Act is to ensure that providers who were aware of AVM on their services but who nevertheless failed to remove the material expeditiously ought to be punishable under law. As currently drafted in s474.34, the (punishable) fault element of recklessness already applies when a provider's service can be used to access AVM, irrespective of whether the provider acted expeditiously to remove the material.	Amend s474.34 to the effect that a provider is only deemed reckless if they have failed to expeditiously remove the AVM from being accessible on their services.	**Amend s474.34 (4) to be:** The fault element for paragraphs (1)(a), (b), (c) and (d) applying in combination is recklessness. *(or similar)* **Amend s474.34 (8) to be:** The fault element for paragraphs (1)(a), (b), (c) and (d) applying in combination is recklessness. *(or similar)*
C	474.35 (5) and (6) and 474.36 (5) and (6) make notices issued by the eSafety Commissioner enforceable by deeming the recipient to have been reckless by virtue of the AVM being accessible on their service. The current approach is not practical because it does not give the notice recipient an opportunity to comply with the notice without exposure to penalty.	We suggest that eSafety Commissioner notices should trigger an obligation to remove the content expeditiously (as it creates awareness of AVM) but that the presumption of recklessness only applies when a provider fails to remove the material expeditiously upon receipt of the notice. This obligation would then, in tandem with our suggested amendments to s474.34, create a regime where providers are deemed	**Delete** from 474.35 the heading "Presumptions" and the current version of 474.35 (5) and (6). **Insert** a new 474.35 (5) to read: (5) On receipt of a notice under subsection (1) issued in relation to a content service by the eSafety Commissioner the provider of the content service must ensure the expeditious removal of the material from the content service. **Insert** a new 474.35 (6) to read: (6) The fault element for paragraph (5) is recklessness. *(Replicate these suggested amendments for s474.36 (i.e. amendment of headline under subsection (6) and replacement of*

		reckless when they are aware of the material but failed to act quickly.	*current subsections (5) and (6) as per the above.)*
<u>Scope includes closed private platforms [concern 2]</u>			
D	B2B infrastructure and cloud providers are private and closed platforms rather than public facing platforms so are a much lower risk for the widespread public dissemination of AVM. They also don't maintain control of the uploaded content like some other public-facing hosts and may be precluded by contractual agreements from reviewing or monitoring content.	We ask that the government consider making minor amendments to provide greater certainty for Australian companies B2B infrastructure and cloud providers could be exempt from being a 'content service' for the purposes of the Act. A new provision could then be added to ensure they are still subject to a notice from the eSafety Commission and would then have an obligation to help remove the material.	**Amend** the definition of "content service" in clause 474.30 by adding at the end: "but this applies only to services provided to the public at the application layer. Cloud and business to business infrastructure is not a content service". Amend the definition of "hosting service" in clause 474.30 by adding at the end of the second sentence: "and include only services provided to the public at the application layer. Cloud and business to business infrastructure is not a hosting service". ***[OR ALTERNATIVELY]*** content service means: (a) a social media service (within the meaning of the Enhancing Online Safety Act 2015); or (b) a designated internet service (within the meaning of the Enhancing Online Safety Act 2015) where the sole or primary purpose of the service is to enable online social interaction between 2 or more end-users. hosting service means a hosting service within the meaning given in the Enhancing Online Safety Act 2015, where the sole or primary purpose of the service is to enable online social interaction between 2 or more end-users. For this purpose, disregard subparagraphs 9C(a)(ii) and (b)(ii) of that Act. Add a clarification to the definition of "hosting services" that:

			Hosting services do not include cloud infrastructure services. Cloud infrastructure services means the provision of on demand physical or virtual resources that provide computing and storage infrastructure capabilities that are independently managed and controlled by another party. **Insert** a new 474.34 (8A) to read: "If for any reason a content service or a hosting service does not ensure the expeditious removal of abhorrent violent material and the eSafety Commissioner has reasonable grounds to believe that the source of the material is a Cloud or business to business infrastructure, upon request from the eSafety Commissioner the operator of the cloud or business to business infrastructure must take reasonable steps to identify and, if possible, remove the material or otherwise prevent it from remaining accessible to the public."
Defences need clarification [concern 3].			
E	**News defence** Section 474.39(1)(e) includes a defence from prosecution under the Act on the basis that "the material relates to a news report, or a current affairs report, that is in the public interest but only where the publication is made by a person working <u>in a professional capacity as a journalist</u>." Considering the speed with which online	We believe some refinements to the defences would help reduce undesired take-down of important and non harmful material. We suggest amending the provision to accommodate online news reporting via social media and other systems that may not involve a journalist.	**Delete** "and" preceding 474.37.(e) (ii): and (ii) is made by a person working in a professional capacity as a journalist; or

	publishers make decisions and the real possibility that the provisions could cover material on important social issues such as lawful protest and police violence, this test should be modified.		
Amendments F-I are simply the implementation of the classifications from E			
F	**Research defence** A defence applies where the accessibility/hosting of material is necessary for, or assistance in, scientific, medical, academic or historical research, but only where the accessibility <u>is reasonable in the circumstances.</u> "Reasonable in the circumstances" creates uncertainty and may be difficult to implement at scale. This qualification introduces significant uncertainty as to whether the defence applies. In practice, it requires providers to be the arbiters of the limits on research. Given the uncertainty, providers may be inclined to remove this material to avoid the risk of committing an offence. This may curb scientific, medical, academic or historical research research.	We believe some refinements to the defences would help reduce undesired take-down of important and non-harmful material. We suggest deleting reference to being "reasonable in the circumstances", while maintaining the intention of this provision.	**Amend** subsection 474.37 (1)(d) as follows ~~Both:~~ ~~(i)~~ the accessibility of the material is necessary for, or of assistance in, conducting scientific, medical, academic or historical research:~~and~~ (~~ii) the accessibility of the material is reasonable in the circumstances for the purpose of conducting that scientific, medical, academic or historical research:~~ or" **Amend** subsection 474.37 (2)(d) as follows: ~~Both~~ ~~(i)~~ the hosting of the material is necessary for, or of assistance in, conducting scientific, medical, academic or historical research; ~~and~~ ~~(ii) the accessibility of the material is reasonable in the circumstances for the purpose of conducting that scientific, medical, academic or historical research:~~ or
G	**Art defence** Accessibility/hosting relates to the development,	We believe some refinements to the defences would help reduce undesired	**Amend** subsection 474.37 (1)(i) as follows:

	performance, exhibition or distribution, <u>in good faith</u>, of an artistic work. It will be extremely difficult for providers to determine the motivations of artists and therefore to form a view as to whether material has been developed "in good faith". This qualification introduces significant uncertainty as to whether the defence applies. In practice, it requires providers to be the arbiters of the intentions of artists and the limits on artistic works. Given the uncertainty, providers may be inclined to remove this material to avoid the risk of committing an offence. This may stymie artistic endeavour.	take-down of important and non-harmful material. We suggest deleting reference to "in good faith" while maintaining the intention of this provision.	(i) the accessibility of the material relates to the development, performance, exhibition or distribution~~, in good faith,~~ of an artistic work. **Amend** subsection 474.37 (2)(i) as follows: (i) the hosting of the material relates to the development, performance, exhibition or distribution~~, in good faith,~~ of an artistic work.
H	**Political expression defence** Accessibility/hosting for purpose of advocating lawful procurement of a change to any matter established by law, policy or practice (e.g. lawful political activism), provided accessibility/hosting is <u>reasonable in the circumstances.</u> "Reasonable in the circumstances" creates uncertainty and may be difficult to implement at scale. This qualification introduces significant uncertainty as to	We believe some refinements to the defences would help reduce undesired take-down of important and non-harmful material. We suggest deleting "and the accessibility of the material is reasonable in the circumstance for that purpose", while maintaining the intention of this provision.	**Amend** 474.37 (2)(h) as follows: (h) the accessibility of the material is for the purpose of advocating the lawful procurement of a change to any matter established by law, policy or practice in: (i) the Commonwealth; or (ii) a State; or (iii) a Territory; or (iv) a foreign country; or (v) a part of a foreign country; ~~and the accessibility of the material is reasonable in the circumstance for that purpose.~~ **Amend** subsection 474.37 (2)(h) as follows: (h)the hosting of the material is for the purpose of advocating the lawful procurement of a change to any

	whether the defence applies. In practice, it requires providers to be the arbiters of the limits on activism. Given the uncertainty, providers may be inclined to remove this material to avoid the risk of committing an offence. This may curb political activism		matter established by law, policy or practice in: (i) the Commonwealth; or (ii) a State; or (iii) a Territory; or (iv) a foreign country; or (v) a part of a foreign country; ~~and the accessibility of the material is reasonable in the circumstances for that purpose~~.
I	**New defence** In high volume social media platforms, it is not possible to immediately identify every posting that may contain an item of AVM. However, as currently drafted the Act defines AVM by reference to the subject matter concerned. Accordingly, a provider that acts with reasonable diligence can be exposed to penalty while undertaking a process for identification and removal.	We propose a defence associated with time taken by administrative and technical processes, to moderate the risk that AVM will be posted and not immediately be identified for removal due to the challenges inherent in locating the material.	**Insert** a new provision 474.37 (1) (J) (j) The content is accessible on the content service for a limited period of time associated with the operation of administrative and technical processes necessary for identification and/or removal. **Insert** a new provision 474.37 (2)(j) (j) The content is accessible on the hosting service for a limited period of time associated with the operation of administrative and technical processes necessary for identification and/or removal.
<u>No formal review process</u> [concern 4]			
J	We appreciate that for a notice to work effectively, it's important for the eSafety Commissioner to act quickly. However, many of the exceptions require questions of judgement, and there is currently no explicit mechanism to rectify mistakes if and when they occur. Currently, the decisions of the eSafety Commissioner are not subject to procedural fairness.	In these circumstances, we believe the decisions of the Commissioner should be subject to review in the fullness of time. We suggest that notices should continue to be binding immediately, with provision for a later review process where necessary. In order to have decisions in relation to AVM subject to administrative	**Insert** 474.41A: "474.41A Review of Decisions of the eSafety Commissioner *Notice issued by the eSafety Commissioner in relation to a content service - review* (1) An application may be made to the Administrative Appeals Tribunal for a review of any decisions made by the eSafety Commissioner to give a content service provider a notice under subsection 474.35 (1).

		review we could amend the *Enhancing Online Safety Act* or insert a provision in the Criminal Code.	*Notice issued by the eSafety Commissioner in relation to a hosting service - review* (1) An application may be made to the Administrative Appeals Tribunal for a review of any decisions made by the eSafety Commissioner to give a hosting service provider a notice under subsection 474.36 (1).”

ADDITIONAL AREAS FOR CONSIDERATION			
<u>Censorship as a result of over compliance</u> [concern 5]			
K	If content is not prohibited by providers' terms of service, but is potentially AVM, many providers may be inclined to remove it, to err on the side of caution given the heavy potential penalties. This is even without a formal notice from the Commissioner. It is also important to promote transparency so the public understands what has been removed.	We propose introducing a formal process whereby a platform can ask the Commissioner for a determination of whether something that is potentially AVM is actually AVM. That decision would then be reviewable. This could be similar to how the Broadcasting Services Act Schedule 7 works with potentially prohibited material.	**Consider amendments to 474.35:** (1) A person who provides a content or hosting service and removes or ceases hosting material that is potentially abhorrent violent material may request that the eSafety Commissioner issue a written notice about that specified material under subsection 474.35(1). (2) If the eSafety Commissioner does not issue a written notice about the material specified in subsection (1) within two weeks, the provider of the content or service may reinstate the specified material, and Subsection 474.34(1) will not apply to that material unless and until a written notice is issued under subsection 474.35(1). (3) In this section, material is 'potential prohibited abhorrent violent material' if: (a) the material has not been subject to a written notice under subsection 474.35(1); and (b) there is a substantial likelihood that the material is abhorrent violent material.
<u>Limited transparency around removal of content</u> [concern 6]			
L	In order to ensure the power to seek a review is meaningful, it may be relevant in some cases to communicate that the take down has been made due to a decision by the eSafety Commissioner.	There could be an option for a notice to be published at the site of the content that is blocked informing interested parties as to why the content is not available (if appropriate).	**Insert** a new provision: 474.36A **Notification of eSafety Commissioner notice to remove**. (a) A content service provider that removes content in accordance with a notification from the eSafety Commissioner under section 474.35 (1) may, if practicable, post a notice at the online location where the content was accessible stating that:

			(i) the content at that was at location has been determined by the eSafety Commissioner to be abhorrent violent material and has been removed in compliance with a notice issued by the eSafety Commissioner under section 474.35(1); and (ii) Any party adversely affected by the decision to take down the material that who considers the material should not have been taken down by reason of an applicable exemption available under s 474.37 of the Criminal Code may appeal to the AAT under section 474.41A of the Criminal Code. (b) a hosting service provider that removes content in accordance with a notification from the eSafety Commissioner under subsection 474.36(1) shall, if practicable, post a notice at the online location where the content was accessible stating that: (i) the content at that was at location has been determined by the eSafety Commissioner to be abhorrent violent material and has been removed in compliance with a notice issued by the eSafety Commissioner under section 474.36(1); and (ii) Any party adversely affected by the decision to take down the material who considers the material should not have been taken down by reason of an applicable exception available under subsection 474.37 of the Criminal Code may appeal to the AAT under section 474.41A of the Criminal Code.
<u>Disproportionate penalties</u> [concern 8].			
M	There are high penalties for failing to or ceasing to remove AVM.	We propose significant penalties apply only for repeat non-compliance.	**Insert** in place of 474.34 (10): (10) A first offence against subsection (1) or (5) committed by a body corporate within any 12 month

	The penalties in the Act are maximums: a court would likely impose something less. A penalty unit is current worth $210 AUD so 500 penalty units is $105,000 AUD. A table of comparative penalties is included in the **Appendix**.	One option is to have a first offence amount of 12,500 penalty units ($2,625,000) which is a sufficient deterrent for an individual. Also if doubled the perpetrator will be penalised twice this amount. **NOTE TO READER:** our suggestions as to the amounts you might include are merely suggestions. Please amend to whatever is considered appropriate.	period is punishable on conviction by a fine of not more than 12,500 penalty units; (10A) A second offence against subsection (1) or (5) committed by a body corporate within 12 months is punishable on conviction by a fine of not more than 25,000 penalty units; (10B) A third and subsequent offence against subsection (1) or (5) committed by a body corporate within 12 months of the first offence is punishable on conviction by a fine of not more than the greater of the following: (a) 50,000 penalty units; (b) 0.1% of the annual domestic turnover of the body corporate during the turnover period of 12 months ending at the end of the month in which the conduct constituting the offence occurred.
<u>Difficulty in identifying a 'threat' of kidnapping</u> [concern 9]			
N	In 474.32 kidnapping under *threat* of violence is included as abhorrent violent conduct. This inclusion is not necessary to prevent dissemination of violent material. Including threats is also inconsistent with the other categories of abhorrent violent conduct, as there is no actual violence required. The lack of actual violence makes implementation of policies to detect and remove AVM significantly more complex for providers. Arguably the significant penalties imposed by the law are not	We propose removing reference to a threat of violence.	**Amend** s474.32(5)(c) to remove "or a threat of violence".

	appropriate to attach to films in the absence of actual violence.		
Hard to apply in practice [concern 9].			
O	The obligation to notify the Federal Police of an offence happening in Australia has an unreasonably low threshold that will be hard to apply in practice.	We propose replacing the threshold with a more objective threshold.	In 474.33 (1)(b) delete "has reasonable grounds to believe" and insert "is aware".

4. Case studies

Case studies setting out practical examples of how these concerns can have significant adverse impacts on the lives of Australians, small, medium and large enterprises are set out below.

DETAIL	**IMAGE** (if relevant)
Case study one: YouTube and proactive monitoring	
Amendment: This case study relates to Amendment A (Concern 1). **Challenges/Impacts:** With more than 500 hours of content uploaded every minute to YouTube, technology is not yet clever enough- even with the most advanced machine learning - to automatically screen all content correctly against set standards without making any mistakes. Some of what makes monitoring through artificial intelligence (AI) tricky is placing an image in context, for example, it may need to be able to distinguish between an incidence of AVM and a scene in a violent movie or a first-person shooter video game. Although AI is improving rapidly, there is still a margin for error and most platforms rely on a mix of human moderators and technology. Even when content has been correctly flagged as AVM, perpetrators are increasingly clever at out-smarting it and can quickly fool an algorithm with a simple change to the piece of content (e.g. by changing the colour or cropping the video/image). This changes the 'fingerprint' of the content and makes it undetectable to the algorithm, making it very difficult for providers to guarantee that they have caught every duplicate of the AVM across their platform even when they are aware of the original piece of AVM. It is possible, for instance, that YouTube could catch 99 versions of a piece of abhorrent violent material, but that one version might slip through the net without YouTube knowing that there is one stray piece of AVM still on the platform. In this instance, despite significant effort and investment, YouTube could be prosecuted (and face significant penalties and / or executive imprisonment) for allowing one version of AVM to remain on the platform despite having no knowledge of it. Importantly, smaller start-up or not for profit content sharing platforms do not have the resources (human or technology) to monitor in the same way that the larger platforms do and are at greater risk of being caught up by the Act despite supporting its intentions.	
Case study two: B2B Cloud and Infrastructure Service Providers	
Amendment: This case study relates to Amendment B (Concern 2). **Challenges/impacts:** B2B Cloud and B2B Infrastructure Service Providers host vast amounts of data for commercial clients (the content providers) including airlines, banks, major retailers. In most cases this data is encrypted and even where the service is a 'managed service' commercial, regulatory and technical restrictions often mean that the cloud provider has no visibility or ability to decrypt the data hosted as the encryption key is generally, and increasingly, held by the commercial client[2]. Under the current Act, the E-Safety Commissioner can serve a written notice on *either* the Content Provider who owns the data or the B2B Cloud or B2B Infrastructure Provider. If the E-Safety Commissioner decides to only serve a notice on the BSB Cloud or Infrastructure Providers to remove content, and they do not hold an encryption key, then the only way in which the Cloud or Infrastructure Provider could respond would be to disable access to the entire site. This could have devastating consequences for other legitimate users of the	

[2] See BYOK (Bring Your Own Key) architecture: https://en.wikipedia.org/wiki/Bring_your_own_encryption

site (e.g. other airline travelers, cash withdrawals, access to medical services), as well as cause substantial commercial damage.

We recommend that the E-Safety Commissioner be first required to serve a notice on the content provider and only if they do not respond or act expeditiously, then a notice be served on the B2B Cloud or Infrastructure Service Provider.

Case study three: Startups in Australia

Overview: This case study relates to all amendment areas.

Challenges/impacts: Regulatory barriers can dramatically affect the decision to found early stage technology companies in Australia and their ability to grow and thrive.

Australia has shown itself capable of producing globally-significant startups that are able to generate millions of users that create content. Canva, for example, has over 15 million monthly active users across the globe.[3]

Yet one area in which we have not yet managed to create a globally relevant business is in social media. This is not for lack of reward - businesses like Facebook, Twitter, Youtube, Instagram, Whatsapp and Snapchat are economic powerhouses at the top of the technology boom in the US, attracting incredible investment and job creation.

The AVM law makes attempting to create such a business in Australia a much less attractive proposition than our international competitors. The threat of heavy sanctions, including jail time, for local founders forces startups into choosing between unacceptable levels of risk or unacceptable levels of costly review and oversight.

Paradoxically, the only businesses able to develop and operate systems to combat such unwanted material are larger organisations with the resources and scale to do so. And while it might be unreasonably costly for those organisations, small startups that are already operating in the margins with extremely limited cash are simply unable to develop and maintain a parallel process of review in order to mitigate risk. In the words of Director of Tech Against Terrorism Adam Hadley in the wake of the Halle shooting incident, “The Big Tech companies have a close relationship with one another… What is more difficult is coordinating activity across hundreds of smaller platforms[4].”

The AVM law essentially closes off one of the most lucrative sectors in the technology boom for local startups, ending the race before it has been run.

Case study four: Abu Ghraib image / Wikipedia

[3] https://techcrunch.com/2019/05/20/graphic-design-platform-canva-valued-at-2-5b-with-new-funds/
[4]https://www.vice.com/en_us/article/zmjgzw/the-german-synagogue-shooters-twitch-video-didnt-go-viral-heres-why?utm_source=Tech+Against+Terrorism&utm_campaign=16119363b8-EMAIL_CAMPAIGN_2019_03_24_07_51_COPY_02&utm_medium=email&utm_term=0_cb464fdb7d-16119363b8-68657015

Overview: This case study relates to Amendment A and H. **Challenges/Impacts:** Under current law, Wikipedia's operators would be criminally responsible for hosting an Encyclopaedia article about the abuse of prisoners at Abu Ghraib (see https://en.wikipedia.org/wiki/Abu_Ghraib_torture_and_prisoner_abuse). The article includes an image of a prisoner, Abdou Hussain Saad Faleh, being tortured—an internationally notorious image that was even featured on the cover of The Economist. The image falls within the definition of Abhorrent Violent Material, and no defences apply.	
Case study five: Holocaust Memorial Museum	
Overview: This case study relates to Amendment A, F and G. **Challenges/Impacts:** The United States Holocaust Memorial Museum hosts images of the kidnapping, murder, and torture of Jews in WWII Europe (see, for example, https://www.ushmm.org/learn/timeline-of-events/1942-1945/liquidation-of-the-lodz-ghetto). Despite their clear historical importance, some of these images may fall within the definition of AVM as they have been captured by perpetrators / accomplices. The Holocaust Memorial Museum would have no defence to criminal liability under current law. Some images, like this one to the right, are difficult to evaluate under current law. Because there are very strong penalties in the law, and there is no formal mechanism for a host to check with the eSafety Commissioner whether an image is actually Abhorrent Violent Material, content hosts like museums in Australia face significant criminal liability and are likely to pre-emptively remove important historical images in order to limit their risk.	

5. Conclusion and next steps

Thank you for considering this matter. We would welcome the opportunity to discuss this with you further.

We would like to reiterate our strong support for the intent of the Act and that we are committed to working with the Australian Government to give effect to the law in a way that ensures those who deliberately or wilfully distribute AVM should be the subject of strong penalties.

We believe the amendments outlined above will improve the government's ability to fulfil its overarching intention, in part through providing clear guidance for industry and stakeholders, while ensuring that those who deliberately or wilfully distribute or host AVM will be subject to the full force of the law.

APPENDIX: Comparison of Penalties

This comparison of penalties is an appendix to the Industry and Civil Society joint group submission to the Inquiry into the AVM Act.

In the table below you will find a selection of relevant offences converted to their AUD equivalent. The conversions were made using sections 4AA-4B of the *Crimes Act 1914 (Cth)*. Under those sections:

- 1 penalty unit = $210 dollars
- A term of imprisonment can be converted to penalty units using the following formula: (maximum term of prison expressed in months) x 5
- Lastly, for body corporates, the maximum pecuniary penalty that can be imposed on a natural person is multiplied by 5.

Offence	Legislative Provision	Maximum Penalty	Conversion to AUD
Murder	*Criminal Code Act 1995* (Cth) section 268.8	Imprisonment for life	$420,000 (natural person) $2,100,000 (body corporate)
Torture	*Criminal Code Act 1995* (Cth) section 268.13	Imprisonment for 25 years	$63,000 (natural person) $315,000 (body corporate)
Rape	*Criminal Code Act 1995* (Cth) section 268.14	Imprisonment for 25 years	$63,000 (natural person) $315,000 (body corporate)

Failure by a person who is suspected of committing (or will commit) a terrorist offence to comply with a police officer's request to give the officer the person's personal details	*Crimes Act 1914* (Cth) section 3UC	20 penalty units	$4,200 (natural person) $21,000 (body corporate)
Failure by an operator of an aircraft or ship to answer a question or produce a document if an AFP officer believes the operator has information or documents relevant to the doing of a terrorist act	*Crimes Act 1914* (Cth) section 3ZQM(4)	60 penalty units	$12,600 (natural person) $63,000 (body corporate)
Publishing a matter that identifies child witnesses or child complainants without leave of the court	*Crimes Act 1914* (Cth) section 15YR	12 months prison, or 60 penalty units, or both.	$12,600 (natural person) $63,000 (body corporate)
Bribery of a foreign public official by a body corporate	*Criminal Code Act 1995* (Cth) section 70.2(5)(a)	100,000 penalty units	$21 million
People smuggling	*Criminal Code Act 1995* (Cth) section 73.1	Imprisonment for 10 years or 1,000 penalty units, or both.	$210,000 (natural person) $1,050,000 (body corporate)
Treason by a body corporate	*Criminal Code Act 1995* (Cth) section 80.1AA (Note 2)	10,000 penalty units.	$2,100,000

Treachery (using force or violence to overthrow the Commonwealth government) by a body corporate.	*Criminal Code Act 1995* (Cth) section 80.1AC (Note 2)	10,000 penalty units.	$2,100,000
Bribery of a Commonwealth public official by a body corporate	*Criminal Code Act 1995* (Cth) section 80.1AC (Note 2)	10,000 penalty units.	$2,100,000
Prohibition of transactions that result in an unacceptable media diversity situation coming into existence	*Broadcasting Services Act 1992* (Cth) section 61AG	20,000 penalty units	$4,200,000
Committing a breach through a transaction without approval if the breach relates to a commercial television broadcasting licence or datacasting transmitter licence	*Broadcasting Services Act 1992* (Cth) section 66(1)(e)	20,000 penalty units	$4,200,000
Providing an international broadcasting service without a licence	*Broadcasting Services Act 1992* (Cth) section 121FG(1)	20,000 penalty units	$4,200,000
Providing a commercial television broadcasting service without a licence	*Broadcasting Services Act 1992* (Cth) section 131	20,000 penalty units	$4,200,000

Where designated communications providers that are body corporates fail to comply with a technical assistance notice or technical capability notice.	*Telecommunications Act 1997* (Cth)section 317ZB	Civil penalty of 47,619 penalty units	$9,999,990
Failing to comply with service provider rules	*Telecommunications Act 1997* (Cth) sections 101(1) and 570(3)(a)	$10 million for each contravention.	$10 million
Contravention by a carrier of a condition of its carrier licence	*Telecommunications Act 1997* (Cth) sections 68(1) and 570(3)(a)	$10 million for each contravention.	$10 million