Friday October 22, 2021

Dr Sean Turner
Committee Secretary
PO Box 6100, Parliament House, Canberra ACT 2600
By email: le.committee@aph.gov.au

Dear Dr. Turner,

We thank you for the extended opportunity to respond to the review of the Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019 (AVM Act) Act to the Parliamentary Joint Committee on Law Enforcement (the Committee).

By way of background, the Digital Industry Group Inc. (DIGI) is a non-profit industry association that advocates for the interests of the digital industry in Australia. DIGI's founding members are Apple, eBay, Facebook, Google, Linktree, Twitter and Yahoo, and its associate members are Redbubble, Change.org and Gofundme. DIGI's vision is a thriving Australian digitally-enabled economy that fosters innovation, a growing selection of digital products and services, and where online safety and privacy are protected.

DIGI's endorsement of joint submission

We want to make clear at the outset that DIGI supports the intent of the AVM Act, and the need for regulation to address pro-terror content. No responsible Internet company wants to host such content, and we have a shared goal with governments in stopping its dissemination – which means continually investing in people, technology and processes that ensure online spaces are safe.

Our submission to this review stands together with, and endorses, the joint submission and proposed amendments to the AVM Act put forward by 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. This group includes Communications Alliance, DIGI, Digital Rights Watch, Google Australia and New Zealand, IBM Australia, Tik Tok and Twitter (The Group).

Opportunities to align drafting with intent

As the AVM Act was drafted and passed within the space of five days, it was not the subject of meaningful consultation with relevant stakeholders including the technology industry, legal and technical experts, news media and civil society. There is an important opportunity in this review, two and a half years after the law's passing, to ensure that the intent of the AVM Act is reflected in its drafting, through the amendments that The Group have put together.

As one example, the updated fact sheet on the AVM Act Attorney-General's Department[1] released in September 2021 states:

[1] Attorney General's Department, "Abhorrent Violent Material Act Fact Sheet", updated September 2021, available at https://www.ag.gov.au/sites/default/files/2021-09/AVM%20_Fact_Sheet%282021%29.PDF

The Act does not require providers to take steps to make themselves aware of abhorrent violent material accessible on their platforms and does not require that providers monitor all content on their platforms.

However, as currently drafted, the AVM Act can be interpreted to confer monitoring obligations on providers because it presumes providers to be "reckless" at the time that a notice is issued by the eSafety Commissioner. This confusion is further reinforced by the associated definition of recklessness, where the fault element of recklessness applies irrespective of whether a provider has acted expeditiously to remove Abhorrent Violent Material or not. Making minor amendments to the wording of the AVM Act, in line with the stated intention above in the fact sheet, is critically important in this review. The Group has made specific amendments to this end, and others, to which DIGI wishes to draw your attention.

Contextualising regulatory approaches

While we agree with the need for regulation to address pro-terror content, we wish to place such regulatory approaches in the context of the voluntary work that industry is already undertaking which provides critical pillars in our defense against such content here in Australia and overseas.

Platform-level work & technology

DIGI members comply with Australian law and swiftly remove content that violates it, across a range of subject matter areas including pro-terror content. In addition, members have policies that define what content and behaviour is prohibited on their services, which are regularly updated to ensure they reflect emerging harms and evolving patterns of abuse. While policies vary depending on the service – and specific questions about those policies are best directed to specific companies – members remove and restrict a range of content covered under the AVM Act. Those policies are enforced in a number of ways including through reporting tools, where end-users can escalate policy-violating content, and through machine learning technology that proactively identifies potentially problematic content before many people have consumed it, both of which generally trigger a human review.

Furthermore, several relevant DIGI members created a shared industry database of unique digital fingerprints, known as "hashes", of known violent terrorist imagery or terrorist recruitment videos that had been removed from their services. Today, that database is used by thirteen companies that are members of the Global Internet Forum to Counter Terrorism (GIFCT). Companies rapidly used this database within hours of the Christchurch terrorist attacks adding over a thousand visually-distinct videos related to the attack to it. Crucially, these hashes were shared with smaller businesses to help stop the proliferation of this content on platforms that may not otherwise have the technology and resourcing of larger companies.

Industry collaboration through the GIFCT[2]

This hash database is one example of industry collaboration that is occurring through the GIFCT, which aims to prevent terrorists from exploiting digital platforms. The GIFCT is an NGO designed to prevent terrorists from exploiting digital platforms. Founded by Facebook, Microsoft, Twitter, and YouTube in 2017, the goals of the GIFCT are threefold: (i) building shared technology to prevent and disrupt the spread of terrorist content online, (ii) conducting and funding research by international experts, and (iii) sharing information and best practices with businesses of all sizes to assist them in

[2] For more information about all of the information in this section, visit the Global Internet Forum to Counter Terrorism (GIFCT) website, available at https://gifct.org/about/

managing this content on their platforms. Since 2017, GIFCT's membership has expanded beyond the founding companies, and it has become an independent organisation led by Nicholas Rasmussen.

As one of several of its workstreams, the GIFCT has developed The Content Incident Protocol (CIP) to respond to emerging and active terrorist events, and assess any potential online content produced and disseminated by those involved in the planning or conducting of the attack. When GIFCT declares the CIP is in force, all hashes of an attacker's content is shared in the GIFCT among its members, and a stream of communication is established between them. The first CIP was activated on October 9 2019, following the shooting in Halle, Germany[3].

Collaboration with the Australian and other governments

The efforts through the GIFCT have evolved in conjunction with the Christchurch Call to Action[4], an initiative that governments, technology platforms, and civil society organisations committed to after the devastating March 2019 Christchurch terrorist attack. In addition to the Christchurch Call, technology companies also signed onto a nine-point plan designed to support industry efforts to eliminate terrorist and violent extremist content online.

Following the devastating Christchurch terrorist attacks, the Australian Government established the Taskforce to Combat Terrorist and Extreme Violent Material Online (the Taskforce). Relevant DIGI members participate in the Taskforce, which provided 30 recommendations on practical, tangible and effective measures and commitments to combat the upload and dissemination of terrorist and extreme violent material, including the development of Australia's Domestic Online Crisis Response Protocol (the Protocol). The Protocol aligns with the GIFCT CIP, and is seen as a domestic implementation of the Christchurch Call. This provides a good example of where industry can successfully collaborate with the Australian Government outside of regulatory mechanisms.

Online Safety Act

Finally, we encourage the Committee to closely review the AVM Act alongside the new Online Safety Act, that was passed into law on June 23, 2021, which contains specific provisions in relation to Abhorrent Violent Material. We ask the Committee to closely examine both Acts, and to use this important review to ensure that there are no overlapping provisions that may create confusion for industry.

Thank you for your consideration of these matters raised in DIGI's submission, and the joint submission by The Group of which DIGI is a signatory. Should you have any questions or wish to discuss the representations in this submission further, please do not hesitate to contact me.

Best regards,

[redacted]

Sunita Bose
Managing Director
Digital Industry Group Inc. (DIGI)

[3] Global Internet Forum to Counter Terrorism (GIFCT) website, available at https://gifct.org/about/
[4] Christchurch Call to Eliminate Terrorise & Violent Extremist Content Online, available at https://www.christchurchcall.com/call.html