From Netsweeper

Netsweeper is Canadian-based technology company that provides carrier-grade web filtering solutions used by ISP's and governments internationally for cybersecurity, regulatory compliance, and children's online protection. We would like to offer a brief submission on the draft Online Safety Bill which essentially reinforces the observations we made during the initial consultation stage.

Netsweeper would like to comment in particular on the "*new power for the eSafety Commissioner to rapidly respond to online crisis events (such as the Christchurch terror attack) by requesting internet service providers block access to terrorist and extreme violent content*" which has been included in the draft Bill.

Netsweeper recognises the proposed **Abhorrent Violent Material (AVM) Blocking Scheme** contained in the Bill as a critically important policy initiative, and congratulates the Australian Government on implementing what will be a world-leading mechanism that we are sure many other countries will soon begin to emulate .

We believe, however, that the implementation of the AVM blocking scheme raises a number of practical issues that will determine how effectively it might operate.

Firstly, there is the challenge of quickly identifying the websites hosting the AVM. The e-Safety Commissioner must know the website/s that host/s the AVM before being able to issue the blocking order that would stop it spreading on the internet. If this relies on the public or the authorities to manually report the sites, then it will be incomplete and too late to stop the spread of the AVM.

Netsweeper would propose that the Australian Government consider the adoption of an AI-Based Categorization Engine to identify AVM websites <u>automatically</u> from the internet traffic of the ISPs.

Such a system could be deployed within the ISPs themselves which would receive a copy of the outgoing web requests to scan for the AVM. When an AVM website is located, the system would immediately generate an alert and email a report to the e-Safety Commissioner for her consideration before issuing the blocking order.

Secondly, there is the challenge of blocking websites simultaneously right across Australia in order to prevent the rapid spread of the AVM. When a blocking order is issued, the ISPs must act to block the sites immediately in order to successfully prevent any downloading and re-posting of the AVM to other websites, whether located in Australia or in another country. This is where any manual process of website blocking, as appears to be proposed, would fail to achieve the objective of the blocking order in the first place i.e. stopping the rapid spread of the AVM around the Internet.

Instead, Australian ISPs should be required install a dedicated filtering system to enforce the AVM block quickly. If the ISPs rely on manually configuring their existing network equipment such as firewalls, routers or DNS servers to implement a blocking order then it could not be done immediately because it would be subject to internal engineering processes (e.g. maintenance window, rollback plan, availability of resources) to avoid

disrupting the network. A centrally-managed automated filtering platform would give the ISPs a tool to block an AVM site quickly without risking the network.

This submission may be made public.

[redacted]

[redacted]
Netsweeper (Australia)
[redacted]
Website: www.netsweeper.com