Fact sheet—Online Safety Reform Proposals—Blocking terrorist material online

What is proposed?

A new Online Safety Act would enable the eSafety Commissioner to direct Internet Service Providers (ISPs) to block domains containing terrorist or extreme violent material, for time limited periods, in the event of an online crisis event.

Why is this needed?

Online services and platforms are being misused to promote violent and extremist actions. This misuse was evident with the terrorist attacks that occurred in Christchurch, New Zealand on 15 March this year. Sadly, the Christchurch attacks were not an isolated event. Exposure to terrorist and extreme violent content can traumatise and harm those who view it. It can also compound the harm experienced by the victims of such actions and contribute to the radicalisation of end-users. It is important that governments and industry work quickly and collaboratively to address the promulgation of this type of extreme content in crisis situations.

In the context of the Christchurch terrorist attacks, the eSafety Commissioner utilised an existing power under the *Telecommunications Act 1997* to direct Australian ISPs to continue to block eight domains still containing the Christchurch material. This cemented the measures voluntarily taken by ISPs to protect Australians from exposure to this material. However, there are shortcomings with the use of this existing power as it is not specifically directed or contained to blocking terrorist or extreme violent content. It will be important for industry and government to be able to work quickly and collaboratively to mitigate the dissemination of terrorist and extreme violent material in crisis situations.

How will it work?

It is proposed that the new Online Safety Act would establish a specific and targeted power for eSafety to direct ISPs to block certain domains containing terrorist or extreme violent material, for time limited periods, in the event of an online crisis event. An 'online crisis event' would be an event that involves terrorist or extreme violent material being disseminated online in a manner likely to cause significant harm to the Australian community, warranting a rapid, coordinated and decisive response by industry and relevant government agencies.

In the first instance, the eSafety Commissioner would issue voluntary notices. ISPs would not be required to respond to a voluntary notice, nor would there be any sanctions for non-compliance. ISPs would be provided with immunity from any civil liability for, or in relation to, an act done by an ISP in compliance with a notice.

However, if there was a need for further action, the voluntary notice scheme would be backed up with a power for the eSafety Commissioner to make mandatory notices that would require action by ISPs. These mandatory notices would be supported by compliance obligations and an enforcement mechanism through the Federal Court. As with the voluntary notices, immunity from civil liability would be provided to ISPs acting in compliance with a notice. The notices would be subject to appropriate appeals, transparency and oversight arrangements to ensure the proper and appropriate use of the power.

This approach — a voluntary notice scheme to be used as a first point of call for the eSafety Commissioner supported by a mandatory notice scheme to be used only as required — would seek to balance the need to need to act rapidly to address online safety concerns during online crisis events with broader principles of freedom of expression.

What kind of content will the proposed new blocking measures apply to?

These proposed new power would apply only to domains containing terrorist or extreme violent material. This power would not be available to block websites on a routine or ongoing basis.

How would this new measure relate to the Abhorrent Violent Material Act?

The proposed blocking measures would complement the existing arrangements in the *Criminal Code Act 1995* for addressing abhorrent and violent material. Under the *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019*, it is an offence for internet service providers, hosting service providers or content service providers that fail to notify the Australian Federal Police within a reasonable time about material relating to abhorrent violent conduct occurring in Australia. It is also an offence for content service providers and hosting services providers that fail to remove access to abhorrent violent material expeditiously where that material is reasonably capable of being accessed within Australia.