

ISP Blocking: facts and falsehoods

24 March 2020

What ISP blocking powers does the eSafety Commissioner have?

The eSafety Commissioner may give written directions to a service provider in connection with any of the Commissioner's functions and powers. This includes giving written directions to internet service providers (ISPs) to block Australian access to material that exposes the community to online terrorist and extreme violent material during crisis events.

When would the eSafety Commissioner consider using these powers?

The eSafety Commissioner, government and industry have developed a protocol for determining when to use these powers, in relation to 'online crisis events'. This would be an event involving terrorist or extreme violent material being shared widely online in a manner likely to cause significant harm to the Australian community. The event would also require a rapid, coordinated and decisive response by industry and relevant government agencies to contain the viral spread of the material.

The protocol establishes detailed criteria, high thresholds and checks and balances to ensure the eSafety Commissioner's powers are used only in very limited and very serious circumstances. Any blocking direction made under the protocol would only be in place for a limited time, to be determined on a case by case basis.

Following the initial blocking period, the eSafety Commissioner could take further action to address the relevant material, in consultation with the ISPs and affected websites.

Would the eSafety Commissioner consult with ISPs and websites?

ISPs were consulted on and agreed to the arrangements for blocking websites under the protocol.

Given the urgent nature of an online crisis event, and the need to prevent terrorist or extreme violent material from going viral, the eSafety Commissioner would reach out to affected websites as soon as possible after making a direction, to encourage them to remove the relevant material and be unblocked.

Does the eSafety Commissioner consider human rights when using these powers?

Yes. The eSafety Commissioner is required to complete a 'statement of compatibility with human rights' when giving a direction. Such a statement would set out how the direction promotes certain rights, for example, the right to protection from national, racial or religious hatred. To the extent that a direction may limit other rights, such as the right to seek, receive and impart information, the statement would explain how it does so in a way that is reasonable, necessary and proportionate.

Has the eSafety Commissioner ever used these powers?

Yes. This was in response to an Australian gunman killing 51 people and injuring 50 others in a terrorist attack on two mosques in Christchurch, New Zealand on 15 March 2019.

The gunman live-streamed the first 17 minutes of the attack. The gunman also posted a 'manifesto' online, expressing hate speech and white supremacist rhetoric. The video and manifesto went viral, rapidly and widely spreading via social media and other online platforms.

The Commissioner's powers were used in September to formalise blocking action already taken by ISPs. This was a temporary, six-month direction which was put in place as an interim measure while government considered longer-term options for addressing misuse of online platforms by perpetrators of terrorism and violent extremism. A different protocol was used for this direction, developed with industry to address the unique circumstances of the block.

What else is government doing to protect Australians from access or exposure to online terrorist and extreme violent material?

In December 2019, the then-Department of Communications and the Arts released a [discussion paper](#) that sets out proposals for online safety legislative reform. One of the reform proposals is for the eSafety Commissioner to have a more specific and targeted power 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. The use of the proposed power would be limited to dealing with online crisis events that involve terrorist or extreme violent material. This power would not be available to block websites on a routine or ongoing basis.