WEBSITE BLOCKING IN AN ONLINE CRISIS EVENT

Overview of legislative requirements and industry arrangements

This overview is designed to assist Australian Internet Service Providers (ISPs) to comply with the relevant legislation and alert them to existing arrangements. It is not intended for content or hosting service providers.

The information provided below does not constitute legal advice.

ISPs must refer abhorrent violent material (AVM) to the Australian Federal Police:

What is the legal basis?

Following the 15 March 2019 Christchurch terrorist attacks, and the viral online spread of the livestreamed attack video and the perpetrator's 'manifesto', the Australian Parliament passed the *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019* (Act).

The Act creates additional offences for internet service providers (ISPs) and content and hosting service providers in relation to a failure to refer and/or to remove specific online content.

When do ISPs have to refer AVM?

The Act places obligations on ISPs, hosting service providers and content service providers to refer the details of abhorrent violent material (AVM) that records or streams abhorrent violent conduct that has occurred, or is occurring, in Australia to the Australian Federal Police (AFP) within a reasonable time of becoming aware of the existence of the material.

A service provider is not required to refer such material where the service provider reasonably believes that details of the material are already known to AFP (for example, if there has already been widespread media reporting about particular material, or if the service provider has already referred the material to the National Centre for Missing or Exploited Children or to Interpol).

How quickly do ISPs have to refer the material to AFP?

The Act does not provide detail as to what constitutes a reasonable time for notifying AFP. In guidance published on its website, the Attorney-General's Department (AGD) notes that this "will depend on the unique circumstances in each case. A range of factors will contribute to an overall determination of "reasonableness"; for example, the type and volume of the material and any complaints received about the material, and the capabilities available to the provider."

Do ISPs have to monitor their networks or customers for AVM?

Section 474.39 of the Act makes clear that an ISP does not provide a content service merely because it supplies a carriage service that enables material to be accessed.

The guidance published by AGD highlights that ISPs are not required to monitor traffic that passes over their networks or their customers' usage behaviours, but only requires ISPs to refer AVM when they become aware of such material being accessible through their service.

How do ISPs notify AFP of AVM?

- Email details to: abhorrent.material@lelink.net.au; or
- Call the AFP Operations Coordination Centre Watch Floor Supervisor: +61 2 6126 7299.

What is Abhorrent Violent Material (AVM)?

Abhorrent violent material is limited to very specific categories of the most egregious, violent audio, visual or audio-visual material produced by a perpetrator or their accomplice.

AVM must stream or record conduct where a person engages in a terrorist act (involving serious physical harm or death of another person), murders or attempts to murder another person, tortures another person, rapes another person or kidnaps another person (where the kidnapping involves violence or the threat of violence). This conduct is referred to as 'abhorrent violent conduct'.

The definition includes video, still images (and series of images) and audio recordings.

The definition does not include material recording animated, re-enacted or fictionalised conduct.

The offences created by the Act only apply to footage of abhorrent violent conduct recorded by the perpetrators or their associates. Footage captured by innocent bystanders or made by a person working in a professional capacity as a journalist is not captured by the offences.

There are other exceptions that allow abhorrent violent conduct to be legally accessible. Refer to Section 474.37 (Defences in respect of abhorrent violent material) of the Act for further details.

What happens to AVM that has been identified?

The Act also requires hosting service providers and content services providers to expeditiously remove from, or cease hosting on, their services AVM that is reasonably capable of being accessed within Australia.

The Australian eSafety Commissioner can issue a notice to formally advise a content service or hosting service provider that their platform can be used to access specified abhorrent violent material.

ISPs must block access to websites if directed to do so:

What is the legal basis?

Section 581(2)A of the *Telecommunications Act 1997* provides that the eSafety Commissioner may give written directions to a carrier or a service provider in connection with any of the Commissioner's functions and powers.

The eSafety Commissioner can give a direction to any Australian ISP to block access to AVM. ISPs receiving a direction to block access to a website specified in the Commissioner's direction must comply with the direction.

The eSafety Commissioner can also give a direction to block access to a website that does not contain AVM, as long as the direction is in connection with any of the Commissioner's functions and powers.

How quickly do ISPs need to block access to a website? And for how long?

Communications Alliance and the eSafety Commissioner have developed the *Protocol (No. 2) Governing ISP Blocking in Online Crisis Events* (Protocol) to set out how a direction to ISPs would work in an online crisis event, including for AVM.

The Protocol sets out the arrangements and process for implementing a direction to block websites hosting terrorist or violent criminal material, including:

- the means of determining which ISPs would be subject to blocking directions, the length of time that the ISPs will be required to implement the blocks, and the process for removing the blocks;
- the process to be used to assess whether the terrorist or violent criminal material is sufficiently serious to warrant a blocking direction, and to identify the domains that are hosting the material;
- guidance on the circumstances in which it is anticipated that this power may be used by the eSafety Commissioner;
- the landing page for the blocks and the method of communicating the notice; and
- to the extent possible, ensure automated notification processes are used to their fullest extent and are as efficient as possible.

A number of Australian ISPs have signed the Protocol.

ISPs that would implement website blocking through their own infrastructure in an online crisis event (i.e. where the blocking is not implemented by an upstream wholesale provider) and that would like to become signatories of the Protocol should contact Communications Alliance (including non-members) at info@commsalliance.com.au or call us on 02 9959 9111.

If you require assistance with matters related to website blocking, please contact your wholesale provider (if applicable) or Communications Alliance.