Online Safety Act 2021

Abhorrent Violent Conduct Powers

Regulatory Guidance

eSC RG 5

Updated January 2025

Australian Government | eSafetyCommissioner

Contents

Overview of this guidance

eSafety is committed to empowering all Australians to have safer, more positive experiences online.

This information is for members of the general public, online industry and other professionals who require further information about the Abhorrent Violent Conduct Powers.

It provides an overview of the powers available to eSafety under the Online Safety Act 2021 (the Act) to prevent Australian internet users from accessing material that promotes, incites, instructs in, or depicts abhorrent violent conduct. These powers protect the Australian community by seeking to prevent the viral, rapid and widespread online distribution of terrorist and extreme violent material, such as the video created by the perpetrator of the March 2019 Christchurch terrorist attack.

This document explains how eSafety will generally interpret and apply the law when using our powers under the Act. All decisions will be made on a case-by-case basis.

Overview of the Abhorrent Violent Conduct Powers

The Act includes a number of powers which allow eSafety to request or require an internet service provider to block material that promotes, incites, instructs in, or depicts abhorrent violent conduct.

A request is communicated by giving a blocking request, while a requirement is communicated by giving a blocking notice.

Before giving a blocking request or a blocking notice, eSafety must be satisfied that the availability of the material online is likely to cause significant harm to the Australian community.

There are several enforcement actions available to eSafety where an internet service provider fails to comply with a blocking notice. These include seeking an injunction or civil penalty where a provider fails to block material in response to a blocking notice.

It is intended that blocking requests and blocking notices will only be given in situations where an online crisis event has been declared by eSafety. This is not a statutory requirement, but is included in a protocol developed by eSafety, Australian internet service providers and the Communications Alliance (an industry body for the Australian communications sector).

The Abhorrent Violent Conduct Powers will operate in tandem with this protocol. The protocol sets out the administrative procedures required to notify providers of a potential online crisis event, including key contacts and notification arrangements.

For information about when eSafety may not use these powers, see **Material that is exempt from eSafety's blocking powers** on page 9.

Key terms

What is 'abhorrent violent conduct?'

Abhorrent violent conduct occurs when a person:

- engages in a violent terrorist act
- murders another person
- attempts to murder another person
- tortures another person
- rapes another person, or
- kidnaps another person using violence or the threat of violence.[1]

The Abhorrent Violent Conduct Powers address material that:

- promotes abhorrent violent conduct
- incites abhorrent violent conduct
- instructs in abhorrent violent conduct, or
- depicts abhorrent violent conduct.[2]

When would there be 'significant harm to the Australian community'?

In considering whether the availability of abhorrent violent conduct material online is likely to cause significant harm to the Australian community, eSafety must consider:

- the nature of the material (for example whether it is live streamed material, or particularly high impact material such as a beheading).
- the number of internet users who are likely to access the material (for example the potential for the material to go viral on the internet).
- any other matters that eSafety considers relevant.[3]

What is an 'online crisis event'?

The eSafety Commissioner can declare an online crisis event when abhorrent violent conduct material is shared or spread online in a manner likely to cause significant harm to the Australian community, in circumstances warranting a rapid, coordinated and decisive response by industry and government.

eSafety receives information from law enforcement, relevant government agencies, online industry and other sources, including members of the public, which may assist in determining whether circumstances should be declared an online crisis event. Any declaration of an online crisis event is made in consultation with relevant government agencies and bodies.

[1]Section 474.32(1) of the Criminal Code Act 1995 (Cth). [2]Section 94 of the Act. [3]Sections 95(4) and 99(4) of the Act. See also clauses 95 and 99 of the Explanatory Memorandum to the Online Safety Bill 2021.

Making the decision to request or require blocking

The giving of a blocking request or blocking notice is at eSafety's discretion. This means eSafety makes the final decision about whether we will take action. Not all situations involving the spread of abhorrent violent conduct material during an online crisis event will require eSafety to take action.

Under the Act, before giving a blocking request or a blocking notice, eSafety must consider whether any of our other powers could be used to minimise the likelihood of the material causing significant harm to the Australian community.[4] For example, eSafety may determine that abhorrent violent conduct material is also Class 1 material and exercise its powers under the Online Content Scheme[5] to require removal of this material from the internet. eSafety may also take into account any other factors we consider relevant when deciding whether to use our blocking powers.

Depending on the circumstances, eSafety may choose to use other removal powers under the Act rather than giving a blocking request or a blocking notice. As noted above, under the Online Content Scheme,[6] eSafety may give a removal notice requiring certain online service providers to remove illegal and restricted material, including material that **advocates a violent terrorist act** and material that promotes, instructs or incites in matters of crime and violence. For more information see the **Online Content Scheme regulatory guidance**.

Alternatively, eSafety may choose to issue notices relating to abhorrent violent material under the Criminal Code 1995 (Cth) (Criminal Code).[7] These are not removal notices but are intended to make certain online service providers aware of abhorrent violent material on or hosted by their services. For guidance on these powers see the abhorrent violent material fact sheet.

There may be occasions when eSafety decides to issue a number of different notices, including a removal notice under the Online Content Scheme,[8] an abhorrent violent material notice under the Criminal Code and a blocking notice under the Abhorrent Violent Conduct Powers.

[4]Sections 95(5) and 99(5) of the Act. [5]Part 9 of the Act. [6]Ibid.
[7]Section 474.35 of the Criminal Code 1995 (Cth) [8]Sections 109 and 110 of the Act.

Approaches to compliance and enforcement

Compliance and enforcement options

Under the Act, eSafety may issue blocking requests[9] and blocking notices.[10]

The two powers will ordinarily be used as part of a two-stage approach designed to give the online industry the opportunity to take quick and voluntary action under a blocking request, before an enforceable blocking notice is given. However, it is at the discretion of eSafety as to whether to give a blocking request or move straight to giving a blocking notice.

When giving a blocking request or a blocking notice, eSafety does not have to observe any procedural fairness requirements.

Blocking requests

What is a blocking request?

A blocking request is a written notification requesting that an internet service provider take one or more specific steps to disable access to particular abhorrent violent conduct material.

Internet service providers are not required to respond to a blocking request, as it is voluntary. As such, there are no sanctions for non-compliance with the request. However, if an internet service provider does not comply with a blocking request, eSafety may give them a blocking notice.

Examples of steps that a provider could be asked to take in response to a blocking request include blocking:

- domain names that provide access to the material
- URLs that provide access to the material
- IP addresses that provide access to the material.[11]

In most cases, eSafety will supply providers with a list of domains to block, rather than IP addresses or URLs. The intention of this is to prevent blocking of an IP address that disables access to more than just the abhorrent violent conduct material. Material at specific URLs may also be better dealt with through more targeted interventions such as removal notices under the Online Content Scheme and abhorrent violent material notices under the Criminal Code. Where blocking at the domain level risks excessive blocking, eSafety will consider use of these alternative powers.

[9]Section 95 of the Act. [10]Section 99 of the Act. [11]Section 95(2) of the Act.

When can a blocking request be given?

It is intended that a blocking request will be given when an online crisis event has been declared by the eSafety Commissioner.

A blocking request can be given when all three criteria are met:

- The material can be accessed using an internet carriage service supplied by an internet service provider.
- eSafety is satisfied that the material depicts, promotes, incites or instructs in abhorrent violent conduct.
- eSafety is satisfied that the availability of the material online is likely to cause significant harm to the Australian community.[12]

Where an internet service provider has been requested to take steps to block a domain or related URL, and the person to whom the domain name is registered is known to eSafety, eSafety must give that person a copy of the blocking request as soon as possible after it is given to the internet service provider. This informs the owner that the request has been made due to abhorrent violent conduct material being available on their domain.

How long can a blocking request be in place?

A blocking request remains in place for a period specified in the request, which must be no longer than 3 months.[13]

The request is designed to be time-limited to minimise adverse effects on blocked domains while still preventing potential significant harms that may result from the spread of abhorrent violent conduct material.

Under the industry protocol related to this guidance, blocking requests will normally be for five days, depending on the nature, scope and severity of the online crisis event.

If a request is about to expire but the material still needs to be blocked, eSafety can give a new blocking request that comes into force immediately after the expiry of the original request.[14]

Can a blocking request be revoked?

eSafety may revoke a blocking request by giving written notice to the internet service provider.[15] This would ordinarily be done if the domain or URL ceases to provide access to the abhorrent violent conduct material, or if eSafety considers enough time has passed to reduce the likelihood that the material will spread to a large number of internet users.

What are the consequences of ignoring a blocking request?

There is no enforcement action which arises from a failure to comply with a blocking request after receiving it.

When a provider complies with a blocking request, the provider will be protected from civil proceedings for anything done in compliance with that request.[16]

[12]Section 95(1) of the Act. [13]Section 96(2) of the Act. [14]Section 96(3) of the Act. [15]Section 97(2) of the Act. [16]Section 221(2)(f) of the Act.

Blocking notices

What is a blocking notice?

A blocking notice is a written notice requiring an internet service provider to take one or more specific steps to disable access to abhorrent violent conduct material.

Examples of steps that a provider could be asked to take include blocking:

- domain names that provide access to the material
- URLs that provide access to the material
- IP addresses that provide access to the material.[17]

In most cases, eSafety will supply providers with a list of domains to block, rather than IP addresses or URLs. The intention of this is to prevent blocking of an IP address that disables access to more than just the abhorrent violent conduct material. Material at specific URLs may also be better dealt with through more targeted interventions such as removal notices under the Online Content Scheme and abhorrent violent material notices under the Criminal Code. Where blocking at the domain level risks excessive blocking, eSafety will consider use of these alternative powers.

When can a blocking notice be given?

It is intended that a blocking notice will be given when an online crisis event has been declared by the eSafety Commissioner.

A blocking notice can be given when three criteria are met:

- The material can be accessed using an internet carriage service supplied by an internet service provider.
- eSafety is satisfied that the material depicts, promotes, incites or instructs in abhorrent violent conduct.
- eSafety is satisfied that the availability of the material online is likely to cause significant harm to the Australian community.[18]

There is no requirement to give a blocking request before a blocking notice. eSafety is able to determine the best course of action according to the circumstances of the particular matter.

Where a blocking notice is given to require an internet service provider to take steps to block a domain or related URL and the registered owner of the domain name is known to eSafety, eSafety must give that person a copy of the blocking notice as soon as possible after it is given to the internet service provider.[19] This informs the owner that the notice has been given due to abhorrent violent conduct material being available on their domain.

[16]Section 221(2)(f) of the Act. [17]Section 99(2) of the Act. [18]Section 99(1) of the Act. [19]Section 102 of the Act.

How long can a blocking notice be in place?

A blocking notice remains in place for a period specified in the notice, which must be no longer than 3 months.[20] The notice is designed to be time-limited to minimise adverse effects on blocked domains while still preventing potential harms that may result from the spread of abhorrent violent conduct material.

Under the protocol related to this guidance, blocking notices will normally be for five days, depending on the nature, scope and severity of the online crisis event.

If a notice is about to expire but the material still needs to be blocked, eSafety can give a new blocking notice that comes into force immediately after the expiry of the original notice.[21]

Can a blocking notice be revoked?

eSafety may revoke a blocking notice by giving written notice to the internet service provider.[22] This would ordinarily be done if the domain or URL ceases to provide access to the abhorrent violent conduct material, or if eSafety considers enough time has passed to reduce the likelihood that the material will spread to a large number of internet users.

What are the penalties for ignoring a blocking notice?

An internet service provider must comply with a requirement under a blocking notice.

Failure to comply with a blocking notice may result in a civil penalty of up to 500 penalty units.[23] eSafety may also consider other enforcement options.

Taking enforcement action

eSafety is empowered under the Act to address material that depicts abhorrent violent conduct through a range of actions. Where appropriate, eSafety takes a graduated approach to enforcement action.

Enforcement options available to eSafety include the following:

- **Accepting an enforceable undertaking**. An enforceable undertaking requires an internet service provider to enter into an agreement with eSafety to ensure compliance with the blocking notice requirements. Once accepted by eSafety, the undertaking can be enforced by a court.[24]
- **Seek an injunction**. An injunction is an order granted by a court to compel an internet service provider to take certain actions, or to refrain from taking certain actions, to comply with the blocking notice requirements.[25]
- **Issue an infringement notice**. Infringement notices are notices that set out the particulars of an alleged contravention and specify an amount to be paid. If it is not paid, eSafety may commence civil penalty proceedings.[26]

[20]Section 100(2) of the Act. [21]Section 100(3) of the Act. [22]Section 101(2) of the Act. [23]Section 103 of the Act. The monetary value of 1 penalty unit is $313 (until 30 June 2026) for individuals. In addition, the maximum penalty ordered against a corporation (which can include online service providers) can be 5 times more than the maximum penalty ordered against an individual. [24]Section 164(1)(j) of the Act. [25]Section 165(1)(j) of the Act. [26]Section 163(1) of the Act.

- **Seek a civil penalty order**. These are court orders that require a person who is found to have contravened a civil penalty provision of the Act to pay a penalty.[27]

When a provider complies with a blocking notice, the provider will be protected from civil proceedings for anything done in compliance with that notice.[28]

Material that is exempt from blocking powers

The Act provides for circumstances where abhorrent violent conduct material is exempt from the blocking request and blocking notice provisions.

The exemptions are limited to circumstances where ongoing access to the material is required for one or more of the following reasons:

- It is necessary to enforce, monitor compliance with, or investigate a contravention of an Australian law (Commonwealth, State and Territory laws) or a law of a foreign country or part of a foreign country.
- It is for the purpose of proceedings in a court or tribunal.
- It is necessary for conducting scientific, medical, academic or historical research, and reasonable in the circumstances for this purpose.
- It is related to a news or current affairs report that is in the public interest and made by a person working in a professional capacity as a journalist.
- It is connected with the performance of a public official's duties or functions (or assisting a public official in relation to those duties or functions) and is reasonable in those circumstances.
- It is for the purpose of advocating the lawful procurement of a change to any matter of law, policy or practice established by Australian law (Commonwealth, State and Territory laws) or the law of a foreign country or part of a foreign country.
- It is related to the development, performance, exhibition or distribution, in good faith, of an artistic work.[29]

Review rights

The decision to give a blocking notice is a reviewable decision. The decision can be reviewed internally by eSafety and externally by the Administrative Review Tribunal[#].

A decision to give a blocking request is not a reviewable decision.

Updated: January 2025

[27]Section 162(1) of the Act. [28]Section 221(2)(g) of the Act. [29]Section 104 of the Act. [#]In October 2024, the new Administrative Review Tribunal (ART) replaced the Administrative Appeals Tribunal (AAT).