



Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019

No. 38, 2019

**An Act to amend the *Criminal Code Act 1995*, and
for related purposes**

Note: An electronic version of this Act is available on the Federal Register of Legislation
(<https://www.legislation.gov.au/>)

Contents

1	Short title.....	1
2	Commencement.....	2
3	Schedules.....	2
	Schedule 1—Sharing of abhorrent violent material	3
	<i>Criminal Code Act 1995</i>	3
	Schedule 2—Obligations of internet service providers and internet content hosts	20
	<i>Criminal Code Act 1995</i>	20



Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019

No. 38, 2019

**An Act to amend the *Criminal Code Act 1995*, and
for related purposes**

[Assented to 5 April 2019]

The Parliament of Australia enacts:

1 Short title

This Act is the *Criminal Code Amendment (Sharing of Abhorrent
Violent Material) Act 2019*.

No. 38, 2019 *Criminal Code Amendment (Sharing of Abhorrent Violent Material)* 1
Act 2019

2 Commencement

- (1) Each provision of this Act specified in column 1 of the table commences, or is taken to have commenced, in accordance with column 2 of the table. Any other statement in column 2 has effect according to its terms.

Commencement information		
Column 1	Column 2	Column 3
Provisions	Commencement	Date/Details
1. The whole of this Act	The day after this Act receives the Royal Assent.	6 April 2019

Note: This table relates only to the provisions of this Act as originally enacted. It will not be amended to deal with any later amendments of this Act.

- (2) Any information in column 3 of the table is not part of this Act. Information may be inserted in this column, or information in it may be edited, in any published version of this Act.

3 Schedules

Legislation that is specified in a Schedule to this Act is amended or repealed as set out in the applicable items in the Schedule concerned, and any other item in a Schedule to this Act has effect according to its terms.

Schedule 1—Sharing of abhorrent violent material

Criminal Code Act 1995

1 At the end of Division 474 of the *Criminal Code*

Add:

Subdivision H—Offences relating to use of carriage service for sharing of abhorrent violent material

474.30 Definitions

In this Subdivision:

abhorrent violent conduct has the meaning given by section 474.32.

abhorrent violent material has the meaning given by section 474.31.

consent means free and voluntary agreement.

content service means:

- (a) a social media service (within the meaning of the *Enhancing Online Safety Act 2015*); or
- (b) a designated internet service (within the meaning of the *Enhancing Online Safety Act 2015*).

hosting service has the same meaning as in the *Enhancing Online Safety Act 2015*. For this purpose, disregard subparagraphs 9C(a)(ii) and (b)(ii) of that Act.

474.31 Abhorrent violent material

- (1) For the purposes of this Subdivision, ***abhorrent violent material*** means material that:
 - (a) is:
 - (i) audio material; or

- (ii) visual material; or
- (iii) audio-visual material;
that records or streams abhorrent violent conduct engaged in
by one or more persons; and
- (b) is material that reasonable persons would regard as being, in
all the circumstances, offensive; and
- (c) is produced by a person who is, or by 2 or more persons each
of whom is:
 - (i) a person who engaged in the abhorrent violent conduct;
or
 - (ii) a person who conspired to engage in the abhorrent
violent conduct; or
 - (iii) a person who aided, abetted, counselled or procured, or
was in any way knowingly concerned in, the abhorrent
violent conduct; or
 - (iv) a person who attempted to engage in the abhorrent
violent conduct.
- (2) For the purposes of this section, it is immaterial whether the
material has been altered.
- (3) For the purposes of this section, it is immaterial whether the
abhorrent violent conduct was engaged in within or outside
Australia.

474.32 Abhorrent violent conduct

- (1) For the purposes of this Subdivision, a person engages in
abhorrent violent conduct if the person:
 - (a) engages in a terrorist act; or
 - (b) murders another person; or
 - (c) attempts to murder another person; or
 - (d) tortures another person; or
 - (e) rapes another person; or
 - (f) kidnaps another person.

Murder

- (2) For the purposes of this section, a person (the **first person**) murders another person if:
- (a) the first person's conduct causes the death of the other person; and
 - (b) the conduct constitutes an offence.

Torture

- (3) For the purposes of this section, a person (the **first person**) tortures another person if:
- (a) the first person inflicts severe physical or mental pain or suffering upon the other person; and
 - (b) the other person is in the custody, or under the control, of the first person; and
 - (c) the pain or suffering does not arise only from, and is not inherent in or incidental to, lawful sanctions that are not inconsistent with the Articles of the International Covenant on Civil and Political Rights (a copy of the English text of which is set out in Schedule 2 to the *Australian Human Rights Commission Act 1986*).

Rape

- (4) For the purposes of this section, a person (the **first person**) rapes another person if:
- (a) the first person sexually penetrates the other person without the consent of the other person; or
 - (b) the first person causes the other person to sexually penetrate the first person without the consent of the other person.

Kidnapping

- (5) For the purposes of this section, a person (the **first person**) kidnaps another person if:
- (a) the first person takes or detains the other person without the other person's consent; and
 - (b) the first person takes or detains the other person in order to:
 - (i) hold the other person to ransom or as a hostage; or

- (ii) murder, torture or rape the other person or a third person; or
- (iii) cause serious harm to the other person or a third person; and
- (c) the taking or detention of the other person involves violence or a threat of violence.

Interpretation

- (6) In this section:

sexually penetrate means:

- (a) penetrate (to any extent) the genitalia or anus of a person by any part of the body of another person or by any object manipulated by that other person; or
- (b) penetrate (to any extent) the mouth of a person by the penis of another person; or
- (c) continue to sexually penetrate as defined in paragraph (a) or (b).

terrorist act has the same meaning as in section 100.1. For this purpose, disregard paragraphs 100.1(2)(b), (d), (e) and (f).

- (7) For the purposes of this section, the genitalia or other parts of the body of a person include surgically constructed genitalia or other parts of the body of the person.

474.33 Notification obligations of internet service providers, content service providers and hosting service providers

- (1) A person commits an offence if:
- (a) the person:
 - (i) is an internet service provider; or
 - (ii) provides a content service; or
 - (iii) provides a hosting service; and
 - (b) the person is aware that the service provided by the person can be used to access particular material that the person has reasonable grounds to believe is abhorrent violent material that records or streams abhorrent violent conduct that has occurred, or is occurring, in Australia; and

- (c) the person does not refer details of the material to the Australian Federal Police within a reasonable time after becoming aware of the existence of the material.

Penalty: 800 penalty units.

- (2) For the purposes of this section:
 - (a) it is immaterial whether the content service is provided within or outside Australia; and
 - (b) it is immaterial whether the hosting service is provided within or outside Australia.
- (3) Subsection (1) does not apply if the person reasonably believes that details of the material are already known to the Australian Federal Police.

Note: A defendant bears an evidential burden in relation to the matters in this subsection: see subsection 13.3(3).

474.34 Removing, or ceasing to host, abhorrent violent material

Content service

- (1) A person commits an offence if:
 - (a) the person provides a content service; and
 - (b) the content service can be used to access material; and
 - (c) the material is abhorrent violent material; and
 - (d) the person does not ensure the expeditious removal of the material from the content service.
- (2) For the purposes of subsection (1), it is immaterial whether the content service is provided within or outside Australia.
- (3) Subsection (1) does not apply to material unless the material is reasonably capable of being accessed within Australia.
- (4) The fault element for paragraphs (1)(b) and (c) is recklessness.

Hosting service

- (5) A person commits an offence if:
 - (a) the person provides a hosting service; and

- (b) material is hosted on the hosting service; and
 - (c) the material is abhorrent violent material; and
 - (d) the person does not expeditiously cease hosting the material.
- (6) For the purposes of subsection (5), it is immaterial whether the hosting service is provided within or outside Australia.
- (7) Subsection (5) does not apply to material unless the material is reasonably capable of being accessed within Australia.
- (8) The fault element for paragraphs (5)(b) and (c) is recklessness.

Penalty for individual

- (9) An offence against subsection (1) or (5) committed by an individual is punishable on conviction by imprisonment for a period of not more than 3 years or a fine of not more than 10,000 penalty units, or both.

Penalty for body corporate

- (10) An offence against subsection (1) or (5) committed by a body corporate is punishable on conviction by a fine of not more than the greater of the following:
- (a) 50,000 penalty units;
 - (b) 10% of the annual turnover of the body corporate during the period (the **turnover period**) of 12 months ending at the end of the month in which the conduct constituting the offence occurred.
- (11) For the purposes of this section, the **annual turnover** of a body corporate, during the turnover period, is the sum of the values of all the supplies that the body corporate, and any body corporate related to the body corporate, have made, or are likely to make, during that period, other than the following supplies:
- (a) supplies made from any of those bodies corporate to any other of those bodies corporate;
 - (b) supplies that are input taxed;
 - (c) supplies that are not for consideration (and are not taxable supplies under section 72-5 of the *A New Tax System (Goods and Services Tax) Act 1999*);

- (d) supplies that are not made in connection with an enterprise that the body corporate carries on.
- (12) For the purposes of subsection (11), it is immaterial whether the supplies were made, or are likely to be made, within or outside Australia.
- (13) Expressions used in subsections (11) and (12) that are also used in the *A New Tax System (Goods and Services Tax) Act 1999* have the same meaning in those subsections as they have in that Act.
- (14) The question whether 2 bodies corporate are related to each other is to be determined for the purposes of this section in the same way as for the purposes of the *Corporations Act 2001*.

When material is removed from a content service

- (15) For the purposes of this section, material is **removed** from a content service if the material is not accessible to any of the end-users using the service.

474.35 Notice issued by eSafety Commissioner in relation to a content service—presumptions

- (1) The eSafety Commissioner may issue a written notice stating that, at the time the notice was issued:
- (a) a specified content service could be used to access specified material; and
 - (b) the specified material was abhorrent violent material.
- (2) The eSafety Commissioner must not issue a notice under subsection (1) unless the eSafety Commissioner is satisfied on reasonable grounds that, at the time the notice was issued:
- (a) the specified content service could be used to access the specified material; and
 - (b) the specified material was abhorrent violent material.
- (3) As soon as practicable after issuing a notice under subsection (1), the eSafety Commissioner must give a copy of the notice to the person who provides the content service concerned.

- (4) The eSafety Commissioner is not required to observe any requirements of procedural fairness in relation to the issue of a notice under subsection (1).

Presumptions

- (5) If:
- (a) a notice under subsection (1) is issued in relation to a content service provided by a person; and
 - (b) in a prosecution of the person for an offence against subsection 474.34(1), it is proven that the content service could be used to access the material specified in the notice at the time the notice was issued;

then, in that prosecution, it must be presumed that the person was reckless as to whether the content service could be used to access the specified material at the time the notice was issued, unless the person adduces or points to evidence that suggests a reasonable possibility that the person was not reckless as to whether the content service could be used to access the specified material at the time the notice was issued.

- (6) If a notice under subsection (1) is issued in relation to a content service provided by a person, then, in a prosecution of the person for an offence against subsection 474.34(1), it must be presumed that, at the time the notice was issued, the person was reckless as to whether the material specified in the notice was abhorrent violent material, unless the person adduces or points to evidence that suggests a reasonable possibility that, at the time the notice was issued, the person was not reckless as to whether the specified material was abhorrent violent material.

Other evidentiary matters

- (7) A document purporting to be a notice issued under subsection (1) must, unless the contrary is established, be taken to be such a notice and to have been properly issued.
- (8) The eSafety Commissioner may certify that a document is a copy of a notice issued under subsection (1).
- (9) Subsections (5), (6) and (7) apply to the certified copy as if it were the original.
-

Application

- (10) This section extends to matters and things outside Australia.

474.36 Notice issued by eSafety Commissioner in relation to a hosting service—presumptions

- (1) The eSafety Commissioner may issue a written notice stating that, at the time the notice was issued:
- (a) specified material was hosted on a specified hosting service; and
 - (b) the specified material was abhorrent violent material.
- (2) The eSafety Commissioner must not issue a notice under subsection (1) unless the eSafety Commissioner is satisfied on reasonable grounds that, at the time the notice was issued:
- (a) the specified material was hosted on the specified hosting service; and
 - (b) the specified material was abhorrent violent material.
- (3) As soon as practicable after issuing a notice under subsection (1), the eSafety Commissioner must give a copy of the notice to the person who provides the hosting service concerned.
- (4) The eSafety Commissioner is not required to observe any requirements of procedural fairness in relation to the issue of a notice under subsection (1).

Presumptions

- (5) If:
- (a) a notice under subsection (1) is issued in relation to a hosting service provided by a person; and
 - (b) in a prosecution of the person for an offence against subsection 474.34(5), it is proven that the material specified in the notice was hosted on the hosting service at the time the notice was issued;
- then, in that prosecution, it must be presumed that the person was reckless as to whether the specified material was hosted on the hosting service at the time the notice was issued, unless the person adduces or points to evidence that suggests a reasonable possibility

that the person was not reckless as to whether specified material was hosted on the hosting service at the time the notice was issued.

- (6) If a notice under subsection (1) is issued in relation to a hosting service provided by a person, then, in a prosecution of the person for an offence against subsection 474.34(5), it must be presumed that, at the time the notice was issued, the person was reckless as to whether the material specified in the notice was abhorrent violent material, unless the person adduces or points to evidence that suggests a reasonable possibility that, at the time the notice was issued, the person was not reckless as to whether the specified material was abhorrent violent material.

Other evidentiary matters

- (7) A document purporting to be a notice issued under subsection (1) must, unless the contrary is established, be taken to be such a notice and to have been properly issued.
- (8) The eSafety Commissioner may certify that a document is a copy of a notice issued under subsection (1).
- (9) Subsections (5), (6) and (7) apply to the certified copy as if it were the original.

Application

- (10) This section extends to matters and things outside Australia.

474.37 Defences in respect of abhorrent violent material

Content service

- (1) Subsection 474.34(1) does not apply to material that can be accessed using a service if:
- (a) the accessibility of the material is necessary for enforcing a law of:
 - (i) the Commonwealth; or
 - (ii) a State; or
 - (iii) a Territory; or
 - (iv) a foreign country; or

- (v) a part of a foreign country; or
- (b) the accessibility of the material is necessary for monitoring compliance with, or investigating a contravention of, a law of:
 - (i) the Commonwealth; or
 - (ii) a State; or
 - (iii) a Territory; or
 - (iv) a foreign country; or
 - (v) a part of a foreign country; or
- (c) the accessibility of the material is for the purposes of proceedings in a court or tribunal; or
- (d) both:
 - (i) the accessibility of the material is necessary for, or of assistance in, conducting scientific, medical, academic or historical research; and
 - (ii) the accessibility of the material is reasonable in the circumstances for the purpose of conducting that scientific, medical, academic or historical research; or
- (e) the material relates to a news report, or a current affairs report, that:
 - (i) is in the public interest; and
 - (ii) is made by a person working in a professional capacity as a journalist; or
- (f) both:
 - (i) the accessibility of the material is in connection with the performance by a public official of the official's duties or functions; and
 - (ii) the accessibility of the material is reasonable in the circumstances for the purpose of performing that duty or function; or
- (g) both:
 - (i) the accessibility of the material is in connection with an individual assisting a public official in relation to the performance of the public official's duties or functions; and
 - (ii) the accessibility of the material is reasonable in the circumstances for the purpose of the individual assisting

- the public official in relation to the performance of the public official's duties or functions; or
- (h) the accessibility of the material is for the purpose of advocating the lawful procurement of a change to any matter established by law, policy or practice in:
 - (i) the Commonwealth; or
 - (ii) a State; or
 - (iii) a Territory; or
 - (iv) a foreign country; or
 - (v) a part of a foreign country;and the accessibility of the material is reasonable in the circumstances for that purpose; or
 - (i) the accessibility of the material relates to the development, performance, exhibition or distribution, in good faith, of an artistic work.

Note: A defendant bears an evidential burden in relation to the matters in this subsection (see subsection 13.3(3)).

Hosting service

- (2) Subsection 474.34(5) does not apply to material that is hosted on a hosting service if:
 - (a) the hosting of the material is necessary for enforcing a law of:
 - (i) the Commonwealth; or
 - (ii) a State; or
 - (iii) a Territory; or
 - (iv) a foreign country; or
 - (v) a part of a foreign country; or
 - (b) the hosting of the material is necessary for monitoring compliance with, or investigating a contravention of, a law of:
 - (i) the Commonwealth; or
 - (ii) a State; or
 - (iii) a Territory; or
 - (iv) a foreign country; or
 - (v) a part of a foreign country; or

- (c) the hosting of the material is for the purposes of proceedings in a court or tribunal; or
- (d) both:
 - (i) the hosting of the material is necessary for, or of assistance in, conducting scientific, medical, academic or historical research; and
 - (ii) the hosting of the material is reasonable in the circumstances for the purpose of conducting that scientific, medical, academic or historical research; or
- (e) the material relates to a news report, or a current affairs report, that:
 - (i) is in the public interest; and
 - (ii) is made by a person working in a professional capacity as a journalist; or
- (f) both:
 - (i) the hosting of the material is in connection with the performance by a public official of the official's duties or functions; and
 - (ii) the hosting of the material is reasonable in the circumstances for the purpose of performing that duty or function; or
- (g) both:
 - (i) the hosting of the material is in connection with an individual assisting a public official in relation to the performance of the public official's duties or functions; and
 - (ii) the hosting of the material is reasonable in the circumstances for the purpose of the individual assisting the public official in relation to the performance of the public official's duties or functions; or
- (h) the hosting of the material is for the purpose of advocating the lawful procurement of a change to any matter established by law, policy or practice in:
 - (i) the Commonwealth; or
 - (ii) a State; or
 - (iii) a Territory; or
 - (iv) a foreign country; or
 - (v) a part of a foreign country;

and the hosting of the material is reasonable in the circumstances for that purpose; or

- (i) the hosting of the material relates to the development, performance, exhibition or distribution, in good faith, of an artistic work.

Note: A defendant bears an evidential burden in relation to the matters in this subsection (see subsection 13.3(3)).

Functions

- (3) The references in this section to function or functions do not, by implication, affect the meaning of the expressions duty or duties when used in any other provision of this Code.

Application

- (4) This section extends to matters and things outside Australia.

474.38 Implied freedom of political communication

- (1) This Subdivision does not apply to the extent (if any) that it would infringe any constitutional doctrine of implied freedom of political communication.
- (2) Subsection (1) does not limit the application of section 15A of the *Acts Interpretation Act 1901* to this Act.

474.39 Provider of content service

- (1) For the purposes of this Subdivision, a person does not provide a content service merely because the person supplies a carriage service that enables material to be accessed.
- (2) For the purposes of this Subdivision, a person does not provide a content service merely because the person provides a billing service, or a fee collection service, in relation to a content service.

474.40 Service of copies of notices by electronic means

Paragraphs 9(1)(d) and (2)(d) of the *Electronic Transactions Act 1999* do not apply to a copy of a notice under subsection 474.35(1) or 474.36(1) of this Act.

Note: Paragraphs 9(1)(d) and (2)(d) of the *Electronic Transactions Act 1999* deal with the consent of the recipient of information to the information being given by way of electronic communication.

474.41 Giving a copy of a notice to a contact person etc.

Contact person

- (1) If:
- (a) a copy of a notice under subsection 474.35(1) is required to be given to the provider of a content service that is a social media service (within the meaning of the *Enhancing Online Safety Act 2015*); and
 - (b) there is an individual who is:
 - (i) an employee or agent of the provider; and
 - (ii) designated as the service's contact person for the purposes of that Act; and
 - (c) the contact details of the contact person have been notified to the eSafety Commissioner;
- the copy of the notice is taken to have been given to the provider if it is given to the contact person.

Agent

- (2) If:
- (a) a copy of a notice under subsection 474.35(1) or 474.36(1) is required to be given to a body corporate incorporated outside Australia; and
 - (b) the body corporate does not have a registered office or a principal office in Australia; and
 - (c) the body corporate has an agent in Australia;
- the copy of the notice is taken to have been given to the body corporate if it is given to the agent.

Other matters

- (3) Subsections (1) and (2) have effect in addition to section 28A of the *Acts Interpretation Act 1901*.

Note: Section 28A of the *Acts Interpretation Act 1901* deals with the service of documents.

474.42 Attorney-General's consent required for prosecution

Offence against section 474.33

- (1) Proceedings for an offence against section 474.33 must not be commenced without the Attorney-General's written consent if:
 - (a) the conduct constituting the alleged offence occurs wholly in a foreign country; and
 - (b) at the time of the alleged offence, the person alleged to have committed the offence is neither:
 - (i) an Australian citizen; nor
 - (ii) a body corporate incorporated by or under a law of the Commonwealth or of a State or Territory.
- (2) However, a person may be arrested for, charged with, or remanded in custody or released on bail in connection with, an offence against section 474.33 before the necessary consent has been given.

Offence against section 474.34

- (3) Proceedings for an offence against section 474.34 must not be commenced without the Attorney-General's written consent.
- (4) However, a person may be arrested for, charged with, or remanded in custody or released on bail in connection with, an offence against section 474.34 before the necessary consent has been given.

474.43 Compensation for acquisition of property

- (1) If the operation of this Subdivision would result in an acquisition of property (within the meaning of paragraph 51(xxxi) of the Constitution) from a person otherwise than on just terms (within the meaning of that paragraph), the Commonwealth is liable to pay a reasonable amount of compensation to the person.
- (2) If the Commonwealth and the person do not agree on the amount of the compensation, the person may institute proceedings in:
 - (a) the Federal Court of Australia; or
 - (b) the Supreme Court of a State or Territory;

for the recovery from the Commonwealth of such reasonable amount of compensation as the court determines.

474.44 This Subdivision does not limit Schedule 5 or 7 to the *Broadcasting Services Act 1992*

This Subdivision does not limit the operation of Schedule 5 or 7 to the *Broadcasting Services Act 1992*.

474.45 Review of this Subdivision

- (1) After the end of the 2-year period beginning at the commencement of this section, the Minister must cause to be conducted a review of the operation of this Subdivision.

Report

- (2) A report of the review must be given to the Minister within 12 months after the end of the 2-year period mentioned in subsection (1).
- (3) The Minister must cause copies of a report under subsection (2) to be tabled in each House of the Parliament within 15 sitting days of that House after the Minister receives the report.

2 Section 475.2 of the *Criminal Code*

Before “Section 15.1”, insert “(1)”.

3 Section 475.2 of the *Criminal Code*

After “Part”, insert “(other than Subdivision H of Division 474)”.

4 At the end of section 475.2 of the *Criminal Code*

Add:

- (2) Section 14.1 (standard geographical jurisdiction) does not apply to an offence against Subdivision H of Division 474.

Schedule 2—Obligations of internet service providers and internet content hosts

Criminal Code Act 1995

1 Section 474.25 of the *Criminal Code* (penalty)

Omit “100 penalty units”, substitute “800 penalty units”.

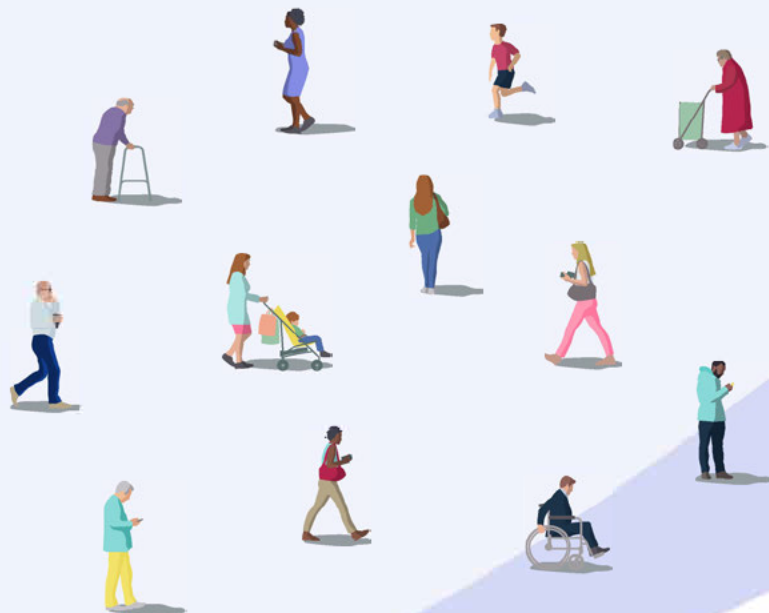
*[Minister’s second reading speech made in—
Senate on 3 April 2019
House of Representatives on 4 April 2019]*

(81/19)

Abhorrent Violent Conduct Powers Regulatory Guidance

eSC RG 5

Updated February 2024



Contents

Overview of this guidance	2
Overview of the Abhorrent Violent Conduct Powers	2
Key terms	3
What is 'abhorrent violent conduct'?	3
When would there be 'significant harm to the Australian community'?	3
What is an 'online crisis event'?	3
Making the decision to request or require blocking	4
Approaches to compliance and enforcement	5
Compliance and enforcement options	5
Blocking requests	5
What is a blocking request?	5
When can a blocking request be given?	6
How long can a blocking request be in place?	6
Can a blocking request be revoked?	6
What are the consequences of ignoring a blocking request?	6
Blocking notices	7
What is a blocking notice?	7
When can a blocking notice be issued?	7
How long can a blocking notice be in place?	8
Can a blocking notice be revoked?	8
What are the penalties for ignoring a blocking notice?	8
Taking enforcement action	8
Material that is exempt from blocking powers	9
Review rights	9

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.

¹Section 474.32(1) of the Criminal Code Act 1995 (Cth). ²Section 94 of the Act. ³Sections 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 Scheme⁵ 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.



⁴Sections 95(5) and 99(5) of the Act. ⁵Part 9 of the Act. ⁶Ibid.

⁷Section 474.35 of the Criminal Code 1995 (Cth) ⁸Sections 109 and 110 of the Act.

Approaches to compliance and enforcement

Compliance and enforcement options

Under the Act, eSafety may issue blocking requests⁹ 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.

⁹Section 95 of the Act. ¹⁰Section 99 of the Act. ¹¹Section 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

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



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

²⁰Section 100(2) of the Act. ²¹Section 100(3) of the Act. ²²Section 101(2) of the Act. ²³Section 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. ²⁴Section 164(1)(j) of the Act.

²⁵Section 165(1)(j) of the Act. ²⁶Section 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 Appeals Tribunal.

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

²⁷Section 162(1) of the Act. ²⁸Section 221(2)(g) of the Act. ²⁹Section 104 of the Act.



s 22

From: Toby Dagg s 22
Sent: 17 April 2024
To: s 47F >
Subject: Re: Time to talk this afternoon? [SEC=OFFICIAL]

OFFICIAL

Hi s 47F

Thanks for your time just now to discuss the state of play in relation to X Corp's response to the eSafety Commissioner's class 1 removal notice, issued yesterday at 2.35pm.

You noted in the call that X Corp. is seeking an extension of time to comply with the notice. Could you please provide this request to me in writing, along with the grounds for why an extension is needed, **by 5.00pm today AEST.**

In addition, you noted that X Corp.'s approach may include geo-blocking the material that is the subject of the class 1 removal notice, but that may not engage the laws of other jurisdictions.

Are you able to confirm whether the approach of geo-blocking is being employed by X Corp. in this instance in response to the class 1 removal notice?

Kind regards,

Toby.

Toby Dagg

General Manager



eSafety acknowledges the Traditional Custodians of country throughout Australia and their continuing connection to land, waters and community. We pay our respects to Aboriginal and Torres Strait Islander cultures, and to Elders past, present and emerging.

From: s 47F
Sent: 17 April 2024 14:45
To: Toby Dagg <s 22 >
Subject: Re: Time to talk this afternoon? [SEC=OFFICIAL]

yes joining now if ok?

On Wed, Apr 17, 2024 at 1:35 PM Toby Dagg <s 22 > wrote:

OFFICIAL

Hi s 47F. I'm available now.

Does Teams work?

https://teams.microsoft.com/l/meetup-join/19%3ameeting_ZTQzOWQxN2EtNWVlMS00OWE0LWI4MjEtZDgwYjc5OTRiODE5%40thread.v2/0?context=%7b%22Tid%22%3a%22ba2b0386-d947-42bf-bf2d-870f776833ef%22%2c%22Oid%22%3a%22e1f4b5fe-ef8e-44fd-af3a-b6c4348fae14%22%7d

Otherwise, s 22.

From: s 47F
Sent: 17 April 2024 14:33
To: Toby Dagg <s 22 >
Subject: Re: Time to talk this afternoon? [SEC=OFFICIAL]

Hi Toby,

Thank you. May I call? What time works for you?

Kind regards,

s 47F



s 47F

On Wed, 17 Apr 2024 at 11:57, Toby Dagg <s 22> wrote:

OFFICIAL

Hi s 47F

As you know, the eSafety Commissioner issued X Corp. a removal notice yesterday afternoon about 2.35pm in connection with a livestreamed video showing the terror-related stabbing attack against Bishop Emmanuel.

We received an automated response acknowledging service, but we have not heard anything further. The 24 hour compliance period for the notice expires soon and I was wanting to check your availability for a call to discuss X Corp's position.

I also wanted to take this opportunity to clarify that, under section 109 of the Online Safety Act 2021, compliance with the removal notice requires that the material is neither accessible to, nor delivered to, **any** end-users in Australia using the service.

One other thing I wanted to discuss was the experience of our investigations teams with using the law enforcement portal today. This is a channel we have employed frequently – including as recently as the weekend in response to the Bondi Junction attack -- to make notifications and flag material of concern on X.

Today, we have found our ability to use the channel obstructed by the need to solve multiple puzzles. These need to be successfully completed before any submission can be made. One eSafety investigator was led through the process a total of ten times before being able to submit the form. We are now experiencing instability with the form. Can you advise why this is the case? Given

that the portal is for law enforcement and government requests the requirement for ease of use is very high.

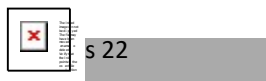
Thanks, and hoping we can urgently talk.

Toby.

Toby Dagg

General Manager

Regulatory Operations Group



eSafety acknowledges the Traditional Custodians of country throughout Australia and their continuing connection to land, waters and community. We pay our respects to Aboriginal and Torres Strait Islander cultures, and to Elders past, present and emerging.

NOTICE: This email message is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the

intended recipient, please contact the sender by reply email and destroy all copies of the original message.

NOTICE: This email message is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender by reply email and destroy all copies of the original message.