EXPLANATORY STATEMENT

Telecommunications (Protecting Australians from Terrorist or Violent Criminal Material) Direction (No. 1) 2019

Telecommunications Act 1997

Prepared by the eSafety Commissioner

The eSafety Commissioner gives the *Telecommunications (Protecting Australians from Terrorist or Violent Criminal Material) Direction (No. 1) 2019* under subsection 581(2A) of the *Telecommunications Act 1997* (the Act).

Subsection 581(2A) of the Act provides that the eSafety Commissioner may give written directions to (a) a carrier or (b) a service provider in connection with performing any of the Commissioner's functions or exercising any of the Commissioner's powers.

This Direction is given in connection with the eSafety Commissioner's function to promote online safety for Australians by protecting Australians from access or exposure to material that promotes, incites, or instructs in, terrorist acts or violent crimes: see *Enhancing Online Safety (Protecting Australians from Terrorist or Violent Criminal Material) Legislative Rule 2019*.

1. Background

The horrific Christchurch terror attack of 15 March 2019, and the subsequent viral dissemination of the perpetrator's video and manifesto (the Christchurch material), demonstrated that there are risks posed to Australian internet users by material involving terrorist acts or violent crime. These risks include direct harms such as experiencing trauma or radicalisation from exposure to hate speech, terrorist propaganda and extreme violence; as well as flow-on harms such as the potential to fall victim to a further attack inspired by this type of material and the desire for online notoriety.

In the immediate wake of the attack, four major Australian internet service providers (ISPs)—Optus, Telstra, TPG and Vodafone—voluntarily undertook to block a number of domains known to be providing access to the Christchurch material as an urgent interim measure to protect Australians from exposure to these materials. In the following weeks, two additional major ISPs—Vocus and Foxtel—also began blocking these domains on a voluntary basis. These ISPs then sought guidance from Government about how to manage the situation in the longer term.

In March 2019, the Prime Minister established the Taskforce to Combat Violent Terrorist and Extreme Material Online (Taskforce) to explore avenues for collaboration between industry and Government to prevent the upload and dissemination of this type of material in the future. In June 2019, the Taskforce released a report outlining a number of actions and recommendations for industry and Government (the Taskforce's report).

Recommendation 5.1 of the Taskforce's report stated that the eSafety Commissioner was to consider utilising subsection 581(2A) of the *Telecommunications Act 1997* to direct the ISPs

currently blocking the Christchurch material to maintain these blocks while the feasibility of longer-term arrangements was assessed.

The eSafety Commissioner considers that it is appropriate for her to exercise her power under subsection 581(2A) of the Act, in connection with her function to promote online safety for Australians by protecting Australians from access or exposure to material that promotes, incites, or instructs in, terrorist acts or violent crimes, for the reasons set out below.

2. Purpose of the instrument

The purpose of the *Telecommunications (Protecting Australians from Terrorist or Violent Criminal Material) Direction (No. 1) 2019* is to direct the service providers who are members of the Optus, Telstra, TPG, Vodafone, Vocus or Foxtel groups to block the websites from which the eSafety Commissioner is aware Christchurch material is accessible. These websites, which comprise of domain names and specific URLs, are recorded in the *list of websites hosting terrorist or violent criminal material (No.1)* (list). There are currently eight overseas-based websites on the list, which is based on the original list compiled by industry. The service providers are currently voluntarily blocking these websites.

As a result, on commencement of the *Telecommunications (Protecting Australians from Terrorist or Violent Criminal Material) Direction (No. 1) 2019*, the relevant service providers will be obligated to continue blocking these websites until the instrument's expiry in six months' time.

This will have the effect of preventing an end-user who is located in Australia who is a customer of the relevant service provider from accessing the websites on the list for a period of six months.

At the time of making the *Telecommunications (Protecting Australians from Terrorist or Violent Criminal Material) Direction (No. 1) 2019*, service providers have advised that the only feasible way to block online content is to impose a domain-level block. However, the list contains both the domain name and URL, permitting service providers to only block the specific URL should any technological advancements become available in the future to facilitate this type of block.

Telecommunications (Protecting Australians from Terrorist or Violent Criminal Material) Direction (No. 1) 2019 may have the effect of blocking some content which is not prohibited on at least three of the eight websites. However, on balance, the eSafety Commissioner is satisfied this instrument is proportionate, given:

- the nature of the Christchurch material and the risks, both potential and realised (in the form of copycat attacks), that the Christchurch material presents to the Australian community;
- the websites have been provided an opportunity to remove the material; and
- there is an ongoing opportunity for websites to remove the material which would allow the eSafety Commissioner to remove them from the list (and thus facilitate the unblocking of the website).

Furthermore, while the eSafety Commissioner does not have the capacity to review all of the content available on each website, the eSafety Commissioner is aware that two of the eight

websites are known for providing access to child sexual abuse material; two others are known for providing access to abhorrent violent material; and another is a self-described 'World News, Politics and the Threat of Islam' blog.

The eSafety Commissioner is satisfied that the Christchurch material is material that promotes, incites or instructs in, terrorist acts or violent crimes. This determination is consistent with the Australian Classification Board's classification of the material as Refused Classification pursuant to Schedule 7 of the *Broadcasting Services Act 1992* and in accordance with the National Classification Code's films table items 1(a) (material that depicts violence or abhorrent phenomena in such a way that they offend against the standards of morality, decency and propriety generally accepted by reasonable adults) and item 1(c) (material that promotes, incites or instructs in matters of crime or violence). As such, the Christchurch material has been designated as 'prohibited' online content. The eSafety Commissioner would therefore have the power to issue an enforceable takedown notice to any Australian-based host of the material under clause 47 of Schedule 7 of the *Broadcasting Services Act 1992*.

The eSafety Commissioner is satisfied that limiting access or exposure to the Christchurch material through the *Telecommunications (Protecting Australians from Terrorist or Violent Criminal Material) Direction (No. 1) 2019* promotes online safety by:

- protecting Australians from the trauma or terror reasonably likely to result from viewing the content;
- protecting and preventing the potential radicalisation or contagion effect of Australians who are vulnerable or sympathetic to the attacker's ideology;
- protecting and preventing the likelihood of the material being used as a recruitment or advocacy tool by terrorist groups to incite further violence; and
- reducing the likelihood of this material being used to threaten, harass or abuse Australians generally, and any specific community groups.

The eSafety Commissioner is further satisfied that directing the relevant service providers to continue blocking the Christchurch material will protect the vast majority of Australians from access or exposure to the material on these websites. Based on data provided by the Communications Alliance, it is estimated that a direction given to the service providers who are members of the six ISPs would have the effect of blocking content to between approximately 95.5% and 96.4% of the Australian fixed and mobile internet subscriber base.

3. Operation of the instrument

Paragraph 5 of the *Telecommunications (Protecting Australians from Terrorist or Violent Criminal Material) Direction (No. 1) 2019* directs the relevant service providers listed in the Schedule to block the websites included in the list of websites hosting terrorist or violent criminal material (No.1) from time to time.

The definitions for the purpose of this instrument are set out in paragraph 4.

Block, in relation to a website, means to implement a mechanism that will prevent access to the website by an end-user located in Australia who is a customer of the relevant service provider.

List of websites hosting terrorist or violent criminal material (No.1) means a list maintained by the eSafety Commissioner in writing of the websites that the Commissioner is satisfied make available material relating to the Christchurch shooting in March 2019 that promotes, incites or instructs in terrorist acts or violent crimes, and from which Australians should be protected from access or exposure.

Subsection 589(2) of the Act provides that an instrument under this Act may make provision in relation to a matter by incorporating matter contained in any other instrument or writing as in force or existing from time to time.

The *List of websites hosting terrorist or violent criminal material (No.1)* (list) is incorporated by reference in accordance with subsection 589(2) of the Act.

This list exists from time to time. The list which exists at the time of making this Direction is based on the original list of domains and URLs compiled by industry, and which are currently being blocked by the relevant service providers. It only includes websites that make available the Christchurch material; websites providing access to other material which promotes, incites or instructs in terrorist acts or violent crimes are not included in this list.

During the six-month period in which this Direction will be in effect, the eSafety Commissioner will review the list on a weekly basis to determine whether the Christchurch material remains available on these URLs. If the Christchurch material is no longer available on a particular URL, this URL will be removed from the list and the relevant service providers will be provided with an updated list.

In furtherance of her mandate to protect Australians from access or exposure to such material, the eSafety Commissioner does not intend to publish this list. This approach is intended to minimise the risk of drawing further attention and traffic to domains whose operators knowingly provide access to the Christchurch material which promotes, incites or instructs in terrorist acts or violent crimes.

Relevant service providers means the service providers listed in the Schedule, who are members of the Optus, Telstra, TPG, Vodafone, Vocus and Foxtel groups.

Following the Christchurch attack, these six service providers undertook to block websites known to be hosting the Christchurch material on a voluntary basis. A direction to these service providers maintains the status quo and, according to data from the industry body, the Communications Alliance, the customers of these service providers account for between 95.5% and 96.4% of the Australian fixed and mobile internet subscriber base.

Terrorist act has the same meaning as in the *Enhancing Online Safety (Protecting Australians from Terrorist or Violent Criminal Material) Legislative Rule 2019*. This, in turn, refers to Part 5.3 of the *Criminal Code* (see section 100.1), under which, at the time of making this instrument, 'terrorist act' means any of the series of actions listed in subsection 100.1(2) of the *Criminal Code*, or threats of those actions, where the action is done or the threat is made with the intention of advancing a political, religious or ideological cause; and the action is done or the threat made with the intention of coercing, or influencing by intimidation, the government of the Commonwealth or a State, Territory or foreign country,

or a part of a State, Territory or foreign country; or intimidating the public or a section of the public.

The actions listed in subsection 100.1(2) include those causing serious harm to persons or property, or serious risk of harm to a person, to health and safety or various critical infrastructure as described in greater detail in the *Criminal Code*. However, the definition excludes, in subsection 100.1(3) of the *Criminal Code*, certain actions taken for advocacy, protest, dissent, industrial action where there was no intent to cause harm.

Violent crime has the same meaning as in the *Enhancing Online Safety (Protecting Australians from Terrorist or Violent Criminal Material) Legislative Rule 2019*. This, in turn, refers to abhorrent violent conduct (within the meaning of Subdivision H of Division 474 of the *Criminal Code*). At the time of making this instrument, a person engages in abhorrent violent conduct if the person engages in a terrorist act; or murders another person; or attempts to murder another person; or tortures another person; or rapes another person; or kidnaps another person.

Paragraph 6 provides that this instrument expires 6 months after it commences, as if it had been repealed by another instrument. The automatic expiry reflects the intention of the eSafety Commissioner that this Direction is an interim measure to protect Australians from exposure to the Christchurch material whilst consideration is given to longer-term measures, including law reform.

4. Consultation

Consultation has taken place with the following:

- Optus, Telstra, TPG, Vodafone, Vocus and Foxtel (collectively, the ISPs), because the relevant service providers subject to this instrument are all members of these ISPs' corporate groups;
- the administrators of the 12 websites that were known to be providing access to the Christchurch material and were therefore proposed to be included in the list of websites hosting terrorist or violent criminal material (No.1) as at 14 August 2019;
- Communications Alliance.

In relation to the administrators of the websites, the purpose of the consultation was to inform them of the eSafety Commissioner's intention to direct the relevant service providers to block their websites and to give them an opportunity to provide any information or feedback on the proposal. It also afforded the websites the opportunity to remove the Christchurch material.

As a result of the consultation process, four website administrators voluntarily took down the Christchurch material from their websites and, accordingly, have been removed from the list.

In our consultation with the ISPs, we asked them to confirm the correct entities for the purpose of the proposed Direction and that these entities were service providers within the meaning of the Act, as well as to provide any feedback on the proposed Direction.

None of the parties consulted raised any objections to the proposed Direction.

The Office of Best Practice Regulation has been consulted and a Regulatory Impact Assessment is not required (OBPR number: 25221)

Statement of Compatibility with Human Rights

Prepared in accordance with Part 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011*

Telecommunications (Protecting Australians from Terrorist or Violent Criminal Material) Direction (No. 1) 2019

Telecommunications (Protecting Australians from Terrorist or Violent Criminal Material) Direction (No. 1) 2019 is compatible with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011*.

Overview

The horrific Christchurch terror attack of 15 March 2019, and the subsequent viral dissemination of the perpetrator's video and manifesto (the Christchurch material), demonstrated that there are risks posed to Australian internet users by material that is streamed or posted online to amplify terrorism and violence.

The eSafety Commissioner's overarching function is to promote Australians' online safety. The eSafety Commissioner also has a specific function, under paragraph 15(1)(r) of the *Enhancing Online Safety Act 2015* and the *Enhancing Online Safety (Protecting Australians from Terrorist or Violent Criminal Material) Legislative Rule 2019*, to protect Australians from access or exposure to material that promotes, incites, or instructs in, terrorist acts or violent crimes.

The purpose of the *Telecommunications (Protecting Australians from Terrorist or Violent Criminal Material) Direction (No. 1) 2019* is to direct the service providers who are members of the Optus, Telstra, TPG, Vodafone, Vocus or Foxtel groups to block the websites from which the eSafety Commissioner is aware Christchurch material is accessible. These websites, which comprise of domains and specific URLs, are recorded in the *list of websites hosting terrorist or violent criminal material (No.1)* (list). There are currently eight overseas-based websites on the list, which is based on the original list compiled by industry. The service providers are currently voluntarily blocking these websites.

The eSafety Commissioner is satisfied that the Christchurch material is material that promotes, incites or instructs in, terrorist acts or violent crimes. This determination is consistent with the Australian Classification Board's classification of the material as Refused Classification pursuant to Schedule 7 of the *Broadcasting Services Act 1992* and in accordance with the National Classification Code's films table items 1(a) (material that depicts violence or abhorrent phenomena in such a way that they offend against the standards of morality, decency and propriety generally accepted by reasonable adults) and item 1(c) (material that promotes, incites or instructs in matters of crime or violence). As such, the Christchurch material is designated as 'prohibited' online content. The eSafety Commissioner would therefore have the power to issue an enforceable takedown notice to any Australian-based host of the material under clause 47 of Schedule 7 of the *Broadcasting Services Act 1992*.

Limiting access or exposure to the Christchurch material through the *Telecommunications (Protecting Australians from Terrorist or Violent Criminal Material) Direction (No. 1) 2019* promotes online safety for Australians by:

- protecting Australians from the trauma or terror reasonably likely to result from viewing the material;
- protecting and preventing the potential radicalisation or contagion effect of Australians who are vulnerable or sympathetic to the attacker's ideology;
- protecting and preventing the likelihood of the material being used as a recruitment or advocacy tool by terrorist groups to incite further violence; and
- reducing the likelihood of this material being used to threaten, harass or abuse Australians generally, and any specific community groups.

Human rights implications

Freedom of opinion and expression

This instrument engages the right to freedom of opinion and expression in article 19 of the *International Covenant on Civil and Political Rights* (ICCPR).

Article 19 of the ICCPR states that a fundamental right is the right "to seek, receive and impart information or ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice".

The right to freedom of opinion and expression is not absolute. Article 19(3) states that this freedom may be subject to special duties and responsibilities. A restriction may occur where it is provided by law and is relevantly necessary for the respect of the rights or reputations of others; or for the protection of national security, public order, or public health or morals.

Telecommunications (Protecting Australians from Terrorist or Violent Criminal Material) Direction (No. 1) 2019 limits the right to freedom of opinion and expression of relevant service providers to provide access to the Christchurch material to their Australian customers. This limitation is aimed at achieving a legitimate objective, and is reasonable, necessary and proportionate.

To the extent that this instrument limits Article 19 of the ICCPR, it does so for the legitimate purpose of protecting Australians from access or exposure to the Christchurch material, being material that is likely to be harmful and offensive to public morals.

There are several features of the Christchurch material which culminate in the need for a targeted enforcement response via this instrument. These include:

- the scale and lethality of the violence depicted;
- the virality in which it was shared across the world;
- the calculated intention by the perpetrator to amplify his agenda and crime through the use of live streaming and the posting of his manifesto online; and

- the apparent potency of the call for others to engage in violence, given that the video and manifesto have been referenced or studied by other perpetrators of violence in the wake of the Christchurch attack.

The effect of this instrument is that the vast majority of Australians will not be able to access the Christchurch material online: The instrument directs service providers who are members of the Optus, Telstra, TPG, Vodafone, Vocus or Foxtel groups to continue blocking the websites known to be providing access to the Christchurch material. Together, they provide internet services to approximately 95.5% and 96.4% of the Australian fixed and mobile internet subscriber base. Therefore, this instrument will achieve the objective of promoting online safety through protecting Australians from access or exposure to material that promotes, incites, or instructs in, terrorist acts or violent crimes.

To the extent that this instrument limits the right to seek, receive and impart information, it does so in a way that is reasonable, necessary and proportionate.

The relevant service providers have advised that, at present, the only feasible way to block the URLs providing access to the Christchurch material is to impose a domain-level block, which means that *Telecommunications (Protecting Australians from Terrorist or Violent Criminal Material) Direction (No. 1) 2019* may have the effect of blocking some content which is not prohibited on at least three of the eight websites. However, on balance, the eSafety Commissioner is satisfied this instrument is proportionate, given:

- the nature of the Christchurch material and the risks, both potential and realised (in the form of copycat attacks), that the Christchurch material presents to the Australian community;
- the websites have been provided an opportunity to remove the material; and
- there is an ongoing opportunity for websites to remove the material which would allow the eSafety Commissioner to remove them from the list (and thus facilitate the unblocking of the website).

Furthermore, while the eSafety Commissioner does not have the capacity to review all of the content available on each website, two of the eight websites are known for providing access to child sexual abuse material; two others are known for providing access to abhorrent violent material; and another is a self-described 'World News, Politics and the Threat of Islam' blog.

There are no other alternative adequate measures for achieving the objective of promoting online safety through protecting Australians from access or exposure to the Christchurch material.

The eSafety Commissioner's powers under Schedule 7 of the *Broadcasting Services Act 1992* to investigate and take down prohibited content are not engaged, because the websites known to be providing access to the Christchurch material are hosted overseas. Similarly, her powers under sections 474.35 and 474.36 of the *Criminal Code Act 1995* in relation to abhorrent violent material are not engaged because the relevant service providers are currently blocking access to the material on a voluntary basis, which means the material is not reasonably capable of being accessed in Australia. It is not possible to issue an access prevention notice under subclause 40(1)(c) of Schedule 5 of the *Broadcasting Services Act 1992* because the power is not available if a code of practice is registered establishing a designated notification scheme: see the Internet and Mobile Content Code. Finally, although

there is a Family Friendly Filter Scheme available, the adequacy and coverage of this scheme means that it is unlikely to cover the majority of Australians.

Right to protection from national, racial, or religious hatred

Article 20(2) of the ICCPR contains mandatory limitations on freedom of expression. It provides that any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility of violence shall be prohibited by law.

This instrument is compatible with Article 20 of the ICCPR, as it seeks to protect Australians from access or exposure to the Christchurch video and manifesto, which advocate national, racial and religious hatred and constitute incitement to discrimination, hostility or violence.

Conclusion

This instrument is compatible with human rights because it promotes the right to protection from national, racial or religious hatred. To the extent that it may limit the right to seek, receive and impart information, it does so in a way that is reasonable, necessary and proportionate to promoting public order, protecting public morals and preserving competing rights.

Julie Inman Grant
eSafety Commissioner