2019 - 2020 - 2021

THE PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA

HOUSE OF REPRESENTATIVES

Online Safety Bill 2021

EXPLANATORY MEMORANDUM

(Circulated by authority of the Minister for Communications, Urban Infrastructure, Cities and the Arts, the Hon Paul Fletcher MP)

ONLINE SAFETY BILL 2021

OUTLINE

The purpose of the Online Safety Bill (the Bill) is to create a new framework for online safety for Australians.

The Bill, together with the Online Safety (Transitional Provisions and Consequential Amendments) Bill 2021, will create a modern, fit for purpose regulatory framework that builds on the strengths of the existing legislative scheme for online safety. In particular, the Bill will:

- retain and replicate provisions in the *Enhancing Online Safety Act 2015* (EOSA) that are working well to protect Australians from online harms, such as the non-consensual sharing of intimate images scheme;
- articulate a core set of basic online safety expectations to improve and promote online safety for Australians;
- reflect a modernised online content scheme to replace the schemes in Schedules 5 and 7 of the *Broadcasting Services Act 1992* (BSA) to address harmful online content;
- create a new complaints-based, removal notice scheme for cyber-abuse being perpetrated against an Australian adult;
- broaden the cyber-bullying scheme to capture harms occurring on services other than social media;
- reduce the timeframe for service providers to respond to a removal notice from the eSafety Commissioner from 48 to 24 hours;
- bring providers of app distribution services and internet search engine services clearly into the remit of the new online content scheme;
- establish a specific and targeted power for the eSafety Commissioner to request or require internet service providers (ISPs) to disable access to material depicting, promoting, inciting or instructing in abhorrent violent conduct, for time-limited periods in crisis situations, reflecting industry's call for Government leadership on this issue.

Online interactions permeate all aspects of modern life and Australians are using the internet to work, to socialise, to consume entertainment and to engage with government, education, health and financial systems. The Government acknowledges that the internet has brought extraordinary economic, social and educational benefits, which each of us enjoy each day. However, these technologies have also provided avenues for those seeking to do harm.

This Bill was developed following substantial public and stakeholder consultation, including consideration of 85 submissions received in response to the public 'Online Safety Legislative Reform Discussion Paper' released in December 2019. An exposure draft of the Bill was released in 2020 and 376 submissions were received.

eSafety Commissioner

Part 2 of the Bill establishes the eSafety Commissioner (the Commissioner) and sets out the Commissioner's functions and powers. The Commissioner will be an independent statutory

office within the Australian Communications and Media Authority (ACMA). A key function of the Commissioner will be to administer: a complaints system for cyber-bullying material targeted at an Australian child; a complaints system for cyber-abuse material targeted at an Australian adult; a complaints and objections system for non-consensual sharing of intimate images; and an online content scheme.

Other functions of the Commissioner will include: promoting online safety for Australians; coordinating relevant activities of Commonwealth Departments, authorities and agencies; supporting, conducting, accrediting and evaluating educational and community awareness programs; making grants; and advising the Minister.

Complaints, objections and investigations system

Part 3 of the Bill establishes complaints system for:

- cyber-bullying material targeted at an Australian child,
- non-consensual sharing of intimate images,
- cyber-abuse material targeted at an Australian adult, and
- an online content scheme.

Complaints system for cyber-bullying material targeted at an Australian child

Complaints can be made to the Commissioner by an Australian child or by a parent or guardian of the child. Other responsible persons can also make a complaint on behalf of an Australian child, if the child authorises them to do so. The Commissioner has the power to investigate complaints and conduct such investigations as the Commissioner sees fit.

Complaints system for non-consensual sharing of intimate images

Complaints or objections can be made to the Commissioner by a person, or an authorised person acting on behalf of that person, if an intimate image of that person has been provided on a social media service, relevant electronic service, or designated internet service without consent.

The Commissioner has the power to investigate complaints and conduct such investigations as the Commissioner sees fit. The Commissioner may also consider whether to give a removal notice to the social media service, relevant electronic service, or designated internet service in relation to the intimate image.

Complaints system for cyber-abuse material targeted at an Australian adult

Complaints can be made to the Commissioner by an Australian adult, or by a responsible person acting with the authorisation of that adult, if cyber-abuse material has been, or is being, provided on a particular social media service, relevant electronic service, or designated internet service.

The Commissioner has the power to investigate complaints and conduct such investigations as the Commissioner sees fit.

Complaints system for the online content scheme

Complaints can be made to the Commissioner if a person believes that:

- end-users in Australia can access class 1 material, or class 2 material covered by paragraph 107(1)(a), (b), (c), (d) or (e), on a social media service, relevant electronic service, or designated internet service; or
- end-users in Australia can access class 2 material covered by paragraph 107(1)(f), (g), (h), (i), (j), (k) or (l) on a particular social media service, relevant electronic service, or designated internet service, and access to the material is not subject to a restricted access system, or
- a person has breached a service provider rule, a civil penalty provision of Part 9, or an industry code or standard under Division 7 of Part 9.

The Commissioner has the power to investigate complaints and conduct such investigations as the Commissioner sees fit.

Basic online safety expectations

Part 4 of the Bill provides that the Minister has the power, by legislative instrument, to determine the basic online safety expectations for social media services, relevant electronic services, or designated internet services.

The Commissioner has the power to prepare and publish a statement on the Commissioner's website stating that a provider of a service has either complied with or contravened one or more basic online safety expectations for that service.

Reporting

Part 4 establishes that the Commissioner has the power to, by written notice, require a provider of a social media service, relevant electronic service, or designated internet service, to prepare and provide reports to the Commissioner about the extent to which the provider complied with one or more specified applicable basic online safety expectations.

A person must comply with a reporting notice from the Commissioner to the extent that the person is capable of doing so. If the social media service, relevant electronic service, or designated internet service fails to do so they will be subject to a civil penalty.

Cyber-bullying material targeted at an Australian child

Part 5 of the Bill establishes a scheme for the rapid removal of cyber-bullying material targeted at an Australian child from a social media service, relevant electronic service, designated internet service or hosting service.

The Commissioner has the power to require a provider of the social media service, relevant electronic service, or designated internet service to remove cyber-bullying material targeted at an Australian child within 24 hours (or such longer period as the Commissioner allows), where certain preconditions are met. These are that: the Commissioner has received a complaint about the material; the material was the subject of a prior complaint to the service provider; the material was not removed from the service within 48 hours after the complaint to the provider was made (or such longer period as the Commissioner allows); and the

Commissioner is satisfied that the material is cyber-bullying material targeted at an Australian child. The Commissioner can also require a hosting service provider to take all reasonable steps to cease hosting the material.

The social media service, relevant electronic service, designated internet service or hosting service provider must comply with the removal notice from the Commissioner to the extent that they are capable of doing so, or be subject to a civil penalty.

End-user notice

Part 5, enables the Commissioner to give an end-user notice to a person who posts cyber-bullying material targeted at an Australian child requiring the person to take all reasonable steps to ensure the removal of the material, refrain from posting further material targeted at the child, or apologise to the child for posting the material.

An injunction will be able to be sought from the Federal Circuit Court for a failure to comply with an end-user notice.

Non-consensual sharing of intimate images

Part 6 of the Bill establishes that posting, or threatening to post, an intimate image of another person on a social media service, relevant electronic service, or designated internet service without the consent of the person depicted in the image is subject to a civil penalty.

Part 6 further establishes a scheme for the removal of such images. The Commissioner has the power, where certain preconditions are met, to require that the provider of the social media service, relevant electronic service, designated internet service, hosting service or the end-user that posted the image, take all reasonable steps to ensure the removal of the image within 24 hours or such longer period as the Commissioner allows.

If the social media service, relevant electronic service, designated internet service, hosting service on which the image has been provided or the end-user that posted the image, fails to remove the image they will be subject to a civil penalty.

Cyber-abuse material targeted at an Australian adult

Part 7 of the Bill establishes a scheme for the removal of cyber-abuse material targeted at an Australian adult from a social media service, relevant electronic service, designated internet service and hosting service.

The Commissioner has the power, where certain preconditions are met, to require that the provider of the social media service, relevant electronic service, designated internet service, hosting service, or the end-user that posted the material on the service, take all reasonable steps to ensure removal of the cyber-abuse material within 24 hours, or such longer period as the Commissioner allows.

A person must comply with a requirement under a removal notice from the Commissioner to the extent that the person is capable of doing so, or be subject to a civil penalty.

Material that depicts abhorrent violent conduct

Part 8 of the Bill establishes that the Commissioner may request or require an internet service provider (ISP) to block access to domain names, URLs or IP addresses containing material that depicts, promotes, incites or instructs in abhorrent violent conduct. Abhorrent violent conduct includes terrorist acts, murder, attempted murder, torture, rape and kidnapping. To issue a blocking request or a blocking notice, the Commissioner must be satisfied that availability of the material online is likely to cause significant harm to the Australian community.

The intent of this power is to prevent the rapid distribution of material online, as occurred, for example, after the 2019 terrorist attacks in Christchurch, New Zealand. It would be used under circumstances where such material is being disseminated online in a manner likely to cause significant harm to the Australian community and that warrants a rapid, coordinated and decisive response by the online industry.

A person must comply with a requirement under a blocking notice to the extent that the person is capable of doing so. If the ISP fails to do so, they will be subject to a civil penalty .

Online content scheme

Part 9 of the Bill establishes a scheme for the removal of class 1 material and class 2 material. This scheme largely replicates the online content scheme in Schedule 5 and Schedule 7 of the BSA, with minimal changes, for example to strengthen the power of the Commissioner in relation to class 1 material provided from, or hosted outside Australia, in certain circumstances.

Class 1 material

The Commissioner has the power to issue a removal notice to the provider of a social media service, relevant electronic service, designated internet service, or hosting service to require the provider take all reasonable steps to ensure the removal of class 1 material on their service where that material can be accessed by end-users in Australia, within 24 hours or such longer period as the Commissioner allows. Class 1 material is defined in the Bill to capture material that would be Refused Classification (RC) if classified under the *Classification (Publications, Films and Computer Games) Act 1995* (the Classification Act).

If the provider of the service fails to remove the material they will be subject to a civil penalty.

Class 2 material

The Commissioner has the power to issue a removal notice to the provider of a social media service, relevant electronic service, or designated internet service that is provided from Australia, to take all reasonable steps to ensure the removal of class 2 material that is covered by paragraph 107(1)(a), (b), (c), (d) or (e) and is or has been provided on their service, within 24 hours, or such longer period as the Commissioner allows. This type of class 2 material is material that would be classified as X 18+, or Category 2 for publications, if the material were classified under the Classification Act. The Commissioner also has a similar power in relation

to hosting service providers regarding material hosted in Australia. If the provider of the service fails to remove the material they will be subject to a civil penalty.

The Commissioner also has the power to issue a remedial notice to a social media service, relevant electronic service or designated service provided from Australia, in relation to class 2 material covered by paragraph 107(1)(f), (g), (h), (i), (j), (k) or (l) that is or has been provided on their service. This type of class 2 material is material that would be rated R 18+ or Category 1 for publications, if the material were classified under the Classification Act. The notice would require the provider to take all reasonable steps to ensure either the material is removed from the service, or that access to the material is subject to a restricted access system. The removal or access restriction must be done within 24 hours or such longer period as the Commissioner allows. The Commissioner also has a similar power in relation to hosting service providers regarding material hosted in Australia. If the provider of the service fails to remove the material they will be subject to a civil penalty.

Link deletion notice

The Commissioner has the power to issue a link deletion notice to the provider of an internet search engine service, to cease providing a link to class 1 material within 24 hours or such longer period as the Commissioner allows, provided certain preconditions are met. These are that the Commissioner is satisfied that there were 2 or more times during the previous 12 months when end-users in Australia could access class 1 material using a link provided by the service and during those 12 months the Commissioner had given at least one removal notice in relation to the material that was not complied with.

Failure to comply with a requirement under a link deletion notice attracts a civil penalty.

App removal notice

The Commissioner has the power to issue an app removal notice to the provider of an app distribution service, to require the provider to cease enabling end-users in Australia to download a particular app that facilitates the posting of class 1 material within 24 hours or such longer period as the Commissioner allows, where certain preconditions are met. These preconditions are that the Commissioner is satisfied that there were at least 2 times during the previous 12 months when end-users in Australia could use the service to download the app and during those 12 months the Commissioner had given at least one removal notice in relation to the class 1 material that was not complied with.

Failure to comply with a requirement under an app removal notice attracts a civil penalty.

Industry codes and industry standards

Part 9 provides a framework for the development and enforcement of online industry codes and standards.

Service provider determinations

Part 9 provides a framework for the development and enforcement of service provider determinations.

The Commissioner has the power to determine, by legislative instrument, rules that apply to providers of social media services, relevant electronic services, designated internet services, hosting services, and internet service providers, in relation to each of their respective services.

A person must not contravene a service provider rule that applies to them. If they do so, they will be subject to a civil penalty.

Federal court orders

Part 9 deals with applications by the Commissioner to the Federal Court for Federal Court orders.

Under this Part, the Commissioner has the power to apply to the Federal Court for an order that the provider of a social media service, relevant electronic service, designated internet service or internet carriage service, cease providing that service if there were 2 or more occasions during the previous 12 months on which the person contravened a civil penalty provision under Part 9 of the Act, and as a result of those contraventions, it would be a significant community safety risk for the person to continue providing that service.

Enforcement

Part 10 of the Bill adopts enforcement arrangements set out in the *Regulatory Powers (Standard Provisions) Act 2014* (Regulatory Powers Act) in respect of civil penalties, infringement notices, enforceable undertakings and injunctions for the purposes of the Bill.

Administrative provisions relating to the Commissioner

Part 11 of the Bill sets out administrative provisions relating to the Commissioner, including provisions relating to appointment, employment terms and conditions, supplementary powers, delegation of functions and powers, annual report, requirements on the ACMA to assist the Commissioner and ministerial directions.

Online Safety Special Account

Part 12 of the Bill continues the existence of the Online Safety Special Account.

The Online Safety Special Account may be used for activities that enhance online safety for Australians including: to make grants under paragraph 27(1)(g); to pay remuneration, and other employment-related costs and expenses, for APS employees whose duties relate to the performance of the Commissioner's functions or the exercise of the Commissioner's powers; and any other costs, expenses and other obligations incurred by the Commonwealth in connection with the performance of the Commissioner's functions or the exercise of the Commissioner's powers.

Information gathering powers

Part 13 of the Bill contains provisions relating to the exercise of the Commissioner's information-gathering powers.

The Commissioner will have the power to obtain information about the identity of an end-user and the contact details of an end-user from a social media service, relevant electronic service or designated internet service. This power can only be exercised if the Commissioner believes on reasonable grounds that the person has the end-user identity information or contact details, and the information or contact details are relevant to the operation of the Act. An example of where the power might be exercised would be to facilitate the issuing of an end-user notice.

A person must comply with a requirement under an information gathering notice from the Commissioner to the extent that the person is capable of doing so. If the social media service, relevant electronic service, or designated internet service fails to do so, they will be subject to a civil penalty.

Investigative powers

Part 14 of the Bill contains provisions relevant to the exercise of the Commissioner's investigative powers.

For the purposes of an investigation, the Commissioner has the power to summon a person by written notice to attend before the Commissioner (or a delegate of the Commissioner named in the notice) to produce documents or to answer questions relevant to the matter being investigated. The Commissioner may also summon a person to provide documents or other information to the Commissioner which is relevant to matter being investigated.

Failure to comply with a requirement to answer a question, produce documents or give evidence attracts a civil penalty and is a criminal offence.

Disclosure of information

Part 15 of the Bill enables the Commissioner to disclose information in certain circumstances, including to the Minister, APS employees for the purpose of advising the Minister, Royal Commissions, certain authorities, teachers or school principals, parents or guardians. This Part will enable the Commissioner to disclose information to teachers or school principals, for example, to assist in the resolution of complaints made under the Act, which may be particularly important in cases of cyber-bullying among school children.

Miscellaneous

Part 16 of the Bill deals with miscellaneous matters, such as review of decisions and legislative rules.

FINANCIAL IMPACT STATEMENT

The Bill might have a minor impact on Commonwealth expenditure or revenue. Additional funding for the Office of the eSafety Commissioner to administer the provisions in this Bill was considered in the context of the 2020-21 Budget.

REGULATION IMPACT STATEMENT

1. Executive summary

The Government intends to reform the existing online safety framework in Australia by developing a new online safety Act and expanding the remit of the Office of the eSafety Commissioner (eSafety Commissioner). The proposed new measures would enhance the protections for Australians from online harms, improve industry accountability for the safety of users, and enable the eSafety Commissioner to operate as a strong and effective regulator.

Over the past two decades Australia has been at the forefront of online safety policy and regulation. In 1999, the broadcasting regime was extended to deal with harmful online content, including child abuse material.[1] In 2015, the Government established the world's first Children's eSafety Commissioner to address the particular harms faced by children online. This became the eSafety Commissioner in 2017 when the remit of the office was extended to include all Australians.

The Government's proposed reforms would build on the strengths of our existing legislative framework. Provisions that have been effective in protecting Australians from online harms would be maintained. This includes the image-based abuse scheme, which has been successful in having image-based abuse material removed in more than 80 per cent of cases, despite nearly all websites reported to date being hosted overseas.[2]

The proposed reforms would also update some elements of the legislation underpinning Australia's online safety regime which are out of date and not flexible enough to deal with emerging issues, such as the rise in the number of social media services and the emergence of

[1] Commonwealth law uses the term 'child abuse material' to capture material that depicts or represents the sexual or physical abuse of a person who is or appears to be under 18 years of age.
[2] Department of Communications and the Arts, *Online Safety Legislative Reform: Discussion Paper,* (Canberra: Department of Communications and the Arts, December 2019), p.36, available at: https://www.communications.gov.au/have-your-say/consultation-new-online-safety-act

new media delivery options. In 2018, an independent review of the *Enhancing Online Safety Act 2015* (EOSA) and Schedules 5 and 7 to the *Broadcasting Services Act 1992* (BSA) was conducted by Ms Lynelle Briggs AO (the 2018 Review). The 2018 Review recommended that there be a single up-to-date online safety Act that would allow key elements of the legislative framework to be modernised and improved. The proposed reforms respond to, and have been informed by, the findings and recommendations of the 2018 Review.

The single up-to-date online safety Act would:

- address gaps in our current legislation by articulating a set of basic online safety expectations (BOSE) that would encourage the prevention of online harms by technology firms and digital platforms, and would improve the transparency of actions taken by social media services;
- modernise the online content scheme by updating the service providers regulated under the scheme and broadening its territorial application;
- create a new complaints-based take-down scheme for cyber-abuse being perpetrated against Australian adults;
- broaden the cyber-bullying scheme to capture harms occurring on services other than social media;
- reduce the timeframe for online service providers to respond to a take-down notice from the eSafety Commissioner from 48 to 24 hours;
- bring ancillary service providers, including search engines and app stores, into the remit of the new regulatory framework; and
- establish an ongoing specific and targeted power for the eSafety Commissioner to direct internet service providers (ISPs) to block domains containing terrorist or extreme violent material for time-limited periods in crisis situations.

The proposed measures would have a relatively low regulatory impact on industry and would be of significant benefit to the community. Major digital platforms and ISPs are already meeting expectations outlined in the proposed measures, including responding to take-down notices issued by the eSafety Commissioner within 24 hours in most cases, complying with the eSafety Commissioner's interim content blocking directions and producing transparency reports. The proposed reforms would provide certainty for industry on the Government's expectations by formalising existing practices.

Reforms to the eSafety Commissioner's funding proposed as part of this package would have no regulatory impact.

2. What policy improvements are we seeking to achieve?

Online harms affect all Australians. Online interactions permeate all aspects of modern life and Australians are using the internet to work, to socialise, to consume entertainment and to engage with government, education, health and financial systems. Children, young women, Australians of Aboriginal or Torres Strait Islander descent and those who identify as Lesbian, Gay, Bisexual, Transgender, Queer or Intersex (LGBTQI) are particularly vulnerable to online harms. Aboriginal and Torres Strait Islander persons and people identifying as LGBTQI experience online hate speech at more than double the national average.[3]

[3] eSafety Commissioner, *Online hate speech: Findings from Australia, New Zealand and Europe*, (Sydney: eSafety Commissioner, 2019), p.6, available at: https://www.esafety.gov.au/sites/default/files/2020-01/Hate%20speech-Report.pdf

Reforms to the existing online safety framework aim to protect more Australians from harm, or risk of harm, resulting from exposure to illegal or inappropriate online content or conduct, including during an Online Crisis Event. The reforms seek to improve online safety in Australia by:

- creating a modern, fit-for-purpose regulatory framework that harnesses the strengths of our existing arrangements and holds industry to account for the safety of their products and services; and
- enhancing the capacity of the eSafety Commissioner to administer the revised regulatory framework effectively and efficiently and enable Australians to engage safely online.

Why are we seeking improvements?

It is important to progress these reforms to safeguard internet users as more Australians adopt digital habits and use the internet in their everyday lives. The extent of online activity in Australia was captured by the Australia Communications and Media Authority (ACMA) 2018-19 Communications Report. The report highlighted that, as at May 2019:

- 90 per cent of Australian adults had accessed the internet, with near universal access by those aged 18–34 (99 per cent);
- 63 per cent of Australian adults used social networking to communicate in the last six months;
- Australian adults also participate in a diverse range of online activities: sending and receiving emails; researching or gathering information; and general internet browsing were the most popular activities, all undertaken by 94 per cent of Australians; and
- more than four in five (83 per cent) Australian internet users viewed video content online, while more than three in five (65 per cent) accessed audio content such as internet radio or podcasts.[4]

Increasingly, internet usage is also becoming pervasive for children. In 2018, the eSafety Commissioner found that 81 per cent of children were online by the age of five and 99 per cent of parents with children aged 2 to 17 years reported having an internet connection in the home.[5] The eSafety Commissioner also reported that 6 per cent of pre-schoolers (aged 2 to 5 years) are accessing social media while 20 per cent are accessing multiplayer online games.[6]

Australia's COVID-19 social distancing and isolation measures have led to a further increase in internet usage to allow people to maintain social and economic connections. Research by the eSafety Commissioner on the impact of COVID-19 on Australian adults' online activities and attitudes found that the number of Australian adults using the internet for one or more tasks had increased by 56 per cent during the first few months of the pandemic.[7] Further,

[4] Australian Communications and Media Authority, *2018-19 Communications Report*, (Australia: Australian Communications and Media Authority, February 2020), p.6, available at: : https://www.acma.gov.au/sites/default/files/2020-04/Communications%20report%202018-19.pdf

[5] eSafety Commissioner, *State of Play – Youth, Kids and Digital Dangers*, (Sydney: eSafety Commissioner, May 2018), p8, available at: https://www.esafety.gov.au/sites/default/files/2019-10/State%20of%20Play%20-%20Youth%20kids%20and%20digital%20dangers.pdf

[6] eSafety Commissioner, *Digital Parenting – Supervising pre-schoolers online*, (Sydney: eSafety Commissioner, August 2018), available at: https://www.esafety.gov.au/about-us/research/digital-parenting/supervising-preschoolers-online

[7] eSafety Commissioner, *COVID-19: Impact on Australian adults' online activities and attitudes*, (Sydney: eSafety Commissioner, June 2020) p.2, available at: https://www.esafety.gov.au/sites/default/files/2020-06/Covid-19-impact-on-Australian-adults-online-report.pdf

Australians viewed the internet as essential during the COVID-19 lockdown to purchase groceries, stay in touch with family and friends and to work.[8] The improvements, outlined in the proposed reforms, are sought in order to meet public expectations on online safety and respond to the pervasiveness of internet usage in Australia.

What are the risks we are seeking to mitigate?

New regulatory challenges

Technological developments have presented new and exciting opportunities for Australians to engage online, but they have also presented new risks and regulatory challenges. New forms of online harms have emerged globally as services, businesses, education and social interactions have increasingly become digitised and connected. Today, online harms include cyber-bullying, abusive commentary or 'trolling', non-consensual sharing of intimate images (image-based abuse), child grooming, cyber-flashing, cyberstalking and technology facilitated abuse and the sharing of personal information without consent (doxing).

Further, as internet usage has expanded, Australians have been exposed to harmful content such as footage of terrorist and extreme violent material, child abuse material and extremely violent or sexually explicit content.

Online service providers have taken meaningful action to address and prevent harms from being incurred as more Australians use their products and services. These actions include investing in technology to detect and prevent the dissemination of policy-violating material, and introducing machine learning algorithms that proactively identify potentially problematic content for human review.[9] The 2018 Review, nevertheless, recommended that new arrangements be made for industry to go beyond compliance with minimum standards, and instead meet a new benchmark that includes taking pre-emptive and preventative action to respond to online harms.[10]

The vulnerability of children

The specific vulnerability of children to negative online experiences requires mitigation through reforms to Australia's online safety framework. According to the eSafety Commissioner, 1 in 5 children have experienced cyber-bullying, and the number of complaints made about serious cyber-bullying of Australian children is increasing year on year. In the reporting period 2018-19, the eSafety Commissioner received 531 complaints about cyber-bullying.[11] this represented a substantial increase on complaints received in 2017-18[12] (409 complaints) and 2016-17[13] (305). Further, a survey of parents and carers

[8] Ibid, p.2.
[9] Sunita Bose, *Consultation on a new Online Safety Act – Submission*, (Sydney: Digital Industry Group Inc, February 2020), p.1, available at: https://www.communications.gov.au/sites/default/files/submissions/consultation_on_a_new_online_safety_act_-_submission_-_digi.pdf
[10] Lynelle Briggs, *Report of the Statutory Review of the Enhancing Online Safety Act 2015 and the Review of Schedules 5 and 7 to the Broadcasting Services Act 1992 (Online Content Scheme),* (Canberra: Department of Communications and the Arts, February 2019), p.2 available athttps://www.communications.gov.au/publications/report-statutory-review-enhancing-online-safety-act-2015-and-review-schedules-5-and-7-broadcasting
[11] eSafety Commissioner, *Office of the eSafety Commissioner Annual Report 2018-19*, (Sydney: eSafety Commissioner, September 2019), p.194
[12] eSafety Commissioner, *Office of the eSafety Commissioner Annual Report 2017-18*, (Sydney: eSafety Commissioner, September 2018), p.114
[13] eSafety Commissioner, *Office of the eSafety Commissioner Annual Report 2016-17*, (Sydney: eSafety Commissioner, September 2017), p.105

highlighted that 28 per cent of parents said their child had been contacted online by strangers.[14]

Parents are concerned about the potential harm to children that is caused by negative online experiences. A 2018 survey of parents and carers noted that the three most pressing concerns for parents and carers in relation to their child's safety online were:

- exposure to inappropriate content other than pornography (38 per cent of respondents expressed concern);
- being in contact with strangers (37 per cent); and
- being bullied online (34 per cent).[15]

Improving how young people gain support when experiencing negative online interactions is important. Research has shown that young people aged 8 to 17, while susceptible to negative online experiences, were often unwilling to seek help from parents, carers, educators, digital platforms and authorities, or were unaware that they could seek help in this way. Only 24 per cent of young people who had negative online experiences sought help in a formal way, whilst 71 per cent sough help in an informal capacity.[16]

Modest reforms to the already successful cyber-bullying scheme are needed to further mitigate this harm for all Australians.

The negative impact of online harms on adults

Adults are at risk of harmful online interactions and experiences. In 2017, the remit of the eSafety Commissioner was expanded to include all Australians, recognising the importance of online safety for the community at large, and the impact of evolving digital technology on user behaviour. This expanded remit did not result in all of the schemes overseen by the eSafety Commissioner being extended to cover adults. In particular, the cyber-bullying scheme continues to only be available to children.

Recent statistics on the prevalence of adult cyber-abuse point to a problem that needs to be mitigated through appropriate reforms:

- a 2018 survey commissioned from the Australia Institute found that 39 per cent of adult internet users reported experiencing one or more forms of online harassment.[17]
- in 2018, Amnesty International undertook a poll in Australia on the experiences of women aged between the ages of 18 and 55 and found that three in ten women surveyed had experienced online abuse or harassment, this includes nearly half for respondents aged 18-24. Alarmingly, 37 per cent of women who had experienced online abuse or harassment said that, on at least one occasion, these online experiences had made them feel physically unsafe.[18]

[14] eSafety Research, *Parenting in the Digital Age*, (Sydney: eSafety Commissioner, 2019), p.4, available at: https://www.esafety.gov.au/sites/default/files/2019-07/eSafety%20Research%20Parenting%20Digital%20Age.pdf
[15] eSafety Research, *Parenting in the Digital Age*, p.4.
[16] eSafety Commissioner, *State of Play – Youth, Kids and Digital Dangers* (Sydney: Office of the eSafety Commissioner, May 2018), p.24
[17] The Australia Institute, *Trolls and polls –the economic costs of online harassment and cyberhate*, (Canberra: The Australia Institute, January 2019), p.2, available at: https://www.tai.org.au/sites/default/files/P530%20Trolls%20and%20polls%20-%20surveying%20economic%20costs%20of%20cyberhate%20%255bWEB%255d_0.pdf
[18] Amnesty International, *Australia: Poll Reveals Alarming Impact of Online Abuse Against Women*, (Sydney: Amnesty International, February 2018), available at: https://www.amnesty.org.au/australia-poll-reveals-alarming-impact-online-abuse-women/

- Plan International's 2019 snapshot of social media commentary of sportswomen and sportsmen found that 'more than a quarter of all comments towards sportswomen were sexist, sexualised, belittled women's sports or were otherwise negative in nature';[19] and
- research by the eSafety Commissioner on hate speech found that about one in seven Australians aged 18-65 years had been the target of online hate in the 12 months to August 2019. A further one in four had been a bystander to it. [20] This was usually encountered through online messaging in social media sites such as Facebook and Instagram. Aboriginal or Torres Strait Islander persons and Australians identifying as LGBTQI were more than twice as likely to experience online hate speech which can cause serious harm.[21] The research also found that perpetrators targeted strangers and were motivated by a desire to amuse, harass or embarrass their targets.[22]

Adults also face reputational damage as a result of harassment online. A Pew Research study in 2014 highlighted the significant after-effects of online harassment for adults. According to the research, approximately one-third of those who had been subject to online harassment felt that their reputation had been damaged.[23]

A number of high-profile cases of adult cyber-abuse, particularly against female athletes such as AFLW player Tayla Harris, have highlighted the negative impact of online harms on adults.[24]

The impact of image-based abuse

The eSafety Commissioner reports that image-based abuse or the sharing of intimate images without consent, affects 11 per cent of adult Australians. [25] This is an extremely destructive form of online abuse which can have devastating impacts for victims. Reports of image-based abuse have increased as more Australians have adopted new digital habits during the COVID-19 isolation period, with reports of image-base abuse up 200 per cent in the first few months of the pandemic.[26]

The sharing of intimate images without consent is, at times, linked to intimate partner and family violence, with 1 in 4 female victims reporting that perpetrators of image-based abuse had engaged in threatening behaviour after an image was shared.[27] According to 2017 research by the eSafety Commissioner, image-based abuse is more prevalent amongst certain population groups including Aboriginal or Torres Strait Islander persons (25%), young women (24%), and those who identify as LGBTQI (19%).[28]

---

[19] Plan International, *Snapshot Analysis Social Media Commentary of Sportswomen and Sportsmen*, (Woking UK: Plan International, April 2019), p.2, available at: https://www.plan.org.au/learn/who-we-are/blog/2019/04/24/240419-snapshot-analysis
[20] eSafety Commissioner, *Online hate speech: Findings from Australia, New Zealand and Europe,* (Sydney: eSafety Commissioner, 2019), p.14, available at: https://www.esafety.gov.au/sites/default/files/2020-01/Hate%20speech-Report.pdf
[21] Ibid, p.14.
[22] Ibid, p.6.
[23] Maeve Duggan, Online Harassment, Pew Research Center, October 2014, available at: https://www.pewresearch.org/internet/2014/10/22/online-harassment/
[24] Patrick Wood and James Maasdorp, "Tayla Harris says trolls' social media comments on AFLW photo were 'sexual abuse'", ABC News, March 2019, available at: https://www.abc.net.au/news/2019-03-20/tayla-harris-felt-sexually-abused-aflw-photo-trolls-seven/10919008
[25] "Image-based abuse", Office of the eSafety Commissioner, 2020, available at: https://www.esafety.gov.au/key-issues/image-based-abuse
[26] "$10 million boost to vital eSafety support", The Hon Paul Fletcher MP, Minister for Communications, Cyber Safety and the Arts, 28 June 2020, available at: https://minister.infrastructure.gov.au/fletcher/media-release/10-million-boost-vital-esafety-support
[27] Research@eSafety, *Image-Based Abuse National Survey: Summary Report,* (Sydney: eSafety Commissioner, October 2017), p.6, available at: https://www.esafety.gov.au/sites/default/files/2019-07/Image-based-abuse-national-survey-summary-report-2017.pdf
[28] Ibid, pp.2-4.

Modest reforms to the already successful image-based abuse scheme are needed to further mitigate this harm for all Australians.

The problem of Illegal and harmful content online is extensive and global

Australians are at risk of exposure to illegal and harmful content, particularly content which is hosted outside of Australia. In September 2019, the eSafety Commissioner reported conducting over 12,000 statutory investigations into potentially prohibited online content over the previous financial year under Schedules 5 and 7 of the BSA (the Online Content Scheme). By far the largest category of content investigated under the scheme is online child abuse material. In September 2018, the eSafety Commissioner reported having undertaken more than 8,000 investigations into child abuse content, representing approximately 35,000 images and videos referred for take-down through its networks. The removal of these images helps to reduce the risk of survivors being further victimised. [29]

Investigations by the eSafety Commissioner address only a small part of the global problem of harmful online content. Government agencies, regulators and digital platforms around the world struggle to review and respond to numerous reports of child sexual abuse and other types of harmful content on a daily basis. Further, the international network of online safety hotlines, called INHOPE, tends to focus on addressing the worst of the worst content (such as child abuse material), meaning that some harmful content is not addressed through current arrangements.

Internationally-based digital platforms are investing in technology to detect and prevent the dissemination of policy-violating content, including harmful online content. The Digital Industry Group Inc (DIGI) has highlighted the work being undertaken by platforms to invest in hashing classifiers to report and identify child exploitation material, and proactively identify potentially problematic content for human review. [30] This investment, while promising, is an imperfect solution and is not enough to address this global issue.

The Government is seeking reform that would protect Australians from harmful content, even if that content is hosted overseas.

What is the cost of doing nothing?

Online harms will continue to impact users negatively

Negative online experiences can cause psychological harm and exacerbate social exclusion for vulnerable individuals and groups and may contribute to adverse mental health outcomes for individuals. Without reform, Australians will continue to be exposed to negative online experiences on social media services, and on new and emerging platforms that they use every day.

There is increasing evidence that both face-to-face bullying and cyber-bullying may have lasting effects on young people, including contributing to poor self-esteem and negative

[29] eSafety Commissioner, *Office of the eSafety Commissioner Annual Report 2017-18*, p.127
[30] Bose, "Consultation on a new Online Safety Act – Submission", p.12.

mental health outcomes, depression, anxiety and suicidal ideation.[31] A review of studies of cyber-bullying, self-harm and suicidal behaviour amongst children and young people published between 1996 and 2017 found that having been a victim or perpetrator of cyber-bullying was associated with higher rates of self-harm than for non-victims or non-perpetrators.[32]

A failure to reform Australia's online safety framework would also mean that hate speech would continue to cause harm for individuals who engage online. Hate speech is a growing concern online, with a 2019 study finding that 7 in 10 adults believed that online hate speech was spreading, with the majority of surveyed adults agreeing that more needed to be done to stop its growth.[33] Hate Speech disproportionately impacts minority groups and marginalised Australians. The top three experiences with online hate speech directed at an individual related to a person's political views (21 per cent), religion (20 per cent) and gender (20 per cent).[34] Those identifying as LGBTQI were particularly vulnerable to online harms, with 61 per cent reporting that their sexual orientation was a reason for being the target of online hate.[35]

The negative impacts of online harms for individuals extend to technology-facilitated abuse directed towards women from culturally and linguistically diverse backgrounds. Research conducted by the eSafety Commissioner in 2019 highlighted that instances of technology-facilitated abuse often involved racist trolling, uninvited sexual messages, racist fetishisation and racial abuse.[36] Research conducted in 2017 found that Aboriginal and Torres Strait Islander people were particularly vulnerable to this type of online harm, with Aboriginal and Torres Strait Islander women experiencing image-based abuse at over twice the rate of other Australians (50 per cent compared to 22 per cent).[37] This abuse is likely to exacerbate psychological distress and poor mental health outcomes, which already occur at a higher rate for Aboriginal and Torres Strait Islander women when compared to non-Aboriginal and Torres Strait Islander people.[38]

Online harms will continue to cause economic challenges

Failure to reform Australia's online safety framework would cause adverse economic effects due to the continuation of pressures that are currently placed on medical and mental health services from victims of online harms. A failure to progress reforms would also mean the

[31] Department of Education and Training, *Submission 2 to the Senate* Committee Inquiry on the adequacy *of existing offences in the Commonwealth Criminal Code and of state and territory criminal laws to capture cyberbullying,* (Canberra: Australian Government Department of Education and Training, 2018), p4.
[32] Ann John, Alexander Charles Glendenning, Amanda Marchant, Paul Montgomery, Anne Stewart, Sophie Wood, Keith Lloyd and Keith Hawton, 'Self-Harm, Suicidal Behaviours, and Cyberbullying in Children and Young People: Systematic Review', *Journal of Medical Internet Research,* April 2018.
[33] eSafety Commissioner, *Online hate speech: Findings from Australia, New Zealand and Europe*, (Sydney: eSafety Commissioner, January 2020), p.7, available at: https://www.esafety.gov.au/sites/default/files/2020-01/Hate%20speech-Report.pdf
[34] Ibid, p.8.
[35] Ibid, p.8.
[36] eSafety Research, *eSafety for Women from Culturally and Linguistically Diverse Backgrounds: Summary Report*, (Sydney: eSafety Commissioner, February 2019), p.17, available at: https://www.esafety.gov.au/sites/default/files/2019-07/summary-report-for-women-from-cald-backgrounds.pdf
[37] Nicola Henry, Anastasia Powell and Asher Flynn, "Not just 'revenge pornography': Australian's experience of image-based abuse*", Gendered Violence and Abuse Research Alliance, Centre for Global Research and Centre for Applied Social Research*, May 2017, p.7, available at: https://www.rmit.edu.au/news/all-news/2017/may/not-just-_revenge-porn--image-based-abuse-hits-1-in-5-australian
[38] eSafety Research, *Online safety for Aboriginal and Torres Strait Islander women living in urban areas*, (Sydney: eSafety Commissioner, October 2019), available at: https://www.esafety.gov.au/sites/default/files/2019-10/Online%20safety%20for%20ATSI%20women%20living%20in%20urban%20areas.pdf

economy would continue to suffer lost productivity when victims reduce their participation in the workforce.

Online harassment is widespread in Australia. According to a 2018 survey commissioned from the Australia Institute by independent journalist and researcher Ginger Gorman, 39 per cent of adult internet users reported experiencing one or more forms of online harassment. A further 4 per cent of respondents to this survey reported seeking help from a doctor, psychologist or other health professional due to being a victim of cyberhate or another form of online harassment. [39] Conservative estimates from the Australia Institute have highlighted that online harassment and cyberhate had resulted in $62 million in medical costs and $267 million in lost income for Australians.[40]

Online safety harms costs the Australian economy. The economic cost of online harassment and cyberhate across the population has been projected to be between $330 million and $3.7 billion to date.[41] Research undertaken by PwC in 2018, which highlighted that 20 per cent of students aged between 8 and 17 years of age had been victims of cyber-bullying over a 12 month period, investigated the economic cost of bullying in Australian schools and estimated that these costs totalled $2.3 billion, incurred while the children are in school and for 20 years after school completion, for each individual school year group.[42] This figure includes bullying that has occurred both online and offline.

Online harms will continue to contribute to and exacerbate broader societal issues

A failure to act to reform Australia's online safety arrangements would result in the continued negative impact of online harms on social cohesion in Australia. Hateful content, particularly content targeting minority groups, continues to be widespread on social media, niche websites and online community forums, and restricts the Government's intention for our society to embrace diversity.[43] The types of hateful content that are distributed online may aggravate tensions, spread fear and have the effect of silencing certain segments of the population, therefore undermining Australian democracy.

Hateful content online may contribute to the radicalisation of at-risk individuals or incite real world violence. The internet in Australia has allowed terrorist groups, including far-right groups, to spread their hateful ideologies across the globe. The Australian Security Intelligence Organisation (ASIO) has highlighted that the internet plays an important role in the radicalisation, recruitment, indoctrination and training of future violent extremists and terrorists.[44] Further, the Australian Government's *Living Safe Together* initiative has commented that radicalisation of individuals can occur both face-to-face and also through a virtual environment online where an individual may become part of an online community of people who share their hateful views and ideologies.[45]

[39] "Trolls and polls –the economic costs of online harassment and cyberhate", p.2.
[40] "Trolls and polls –the economic costs of online harassment and cyberhate", p.11.
[41] "Trolls and polls –the economic costs of online harassment and cyberhate", p.11.
[42] "The Economic Cost of Bullying in Australian Schools", PwC, March 2018, p.i, available at: https://www.amf.org.au/media/2505/amf-report-280218-final.pdf
[43] Department of Home Affairs, *Australia's Multicultural Statement*, (Canberra: Australian Government, March 2017), p.4, available at: https://www.homeaffairs.gov.au/mca/Statements/english-multicultural-statement.pdf
[44] Australian Security Intelligence Organisation, *Counter Terrorism*, (Canberra: Australian Security Intelligence Organisation, 2019), available at: https://www.asio.gov.au/counter-terrorism.html
[45] "Living Safe Together, Preventing violent extremism and radicalisation in Australia", Government of Australia, 2015, note 20, p 12.

Community expectations will not be met by industry

Online service providers are investing in improving the safety of their services, yet actions undertaken by digital platforms, ISPs and other relevant industries do not meet the expectation of the Australian community for stronger preventative measures to combat online harms. The eSafety Commissioner's engagement efforts on Safety by Design,[46] submissions to the 2018 Review,[47] and the public consultation process informing the Government's development of the Online Safety Charter have highlighted a community desire for industry to adhere to stronger measures.

Digital platforms have committed to working with government to enhance online safety for users, and have invested in the development of policies, tools, products and resources to keep people safe. This commitment to work with government includes undertaking to bring forward concrete measures to prevent extreme violent content from being disseminated on their services. Nevertheless, some sectors of industry have been slow to meet the community's expectations regarding online safety, and there is scope to improve industry cooperation further.

Civil society organisations, who were consulted on proposals for a new online safety Act, expressed a desire for Government to take a more proactive role in regulating online harms. Yourtown (Kids Helpline) noted that the eSafety Commissioner should not continue to be reliant on voluntary actions of online service providers to address online harms.[48] The Carly Ryan Foundation went further, suggesting that industry had already had opportunities to self-regulate, and that new ways of communication would contribute to a failure of industry to adequately self-regulate in the future.[49]

It is likely, that without reform, the strong expectations of civil society that Australians be supported online, will not be met.

What are the current measures in place?

The current framework underpinning Australia's online safety arrangements are set out in the EOSA, Schedules 5 and 7 to the BSA and the *Criminal Code Amendment (Sharing Abhorrent Violent Material) Act 2019.*

Enhancing Online Safety Act 2015 and Schedules 5 and 7 of the *Broadcasting Services Act 1992*.

[46] eSafety Commissioner, *Safety by Design Overview*, (Sydney: eSafety Commissioner, May 2019), available at: https://www.esafety.gov.au/sites/default/files/2019-10/SBD%20-%20Overview%20May19.pdf

[47] "Report of the Statutory Review of the Enhancing Online Safety Act 2015 and the Review of Schedules 5 and 7 to the *Broadcasting Services Act 1992* (Online Content Scheme), Department of Communications and the Arts, February 2019, available at: https://www.communications.gov.au/publications/report-statutory-review-enhancing-online-safety-act-2015-and-review-schedules-5-and-7-broadcasting

[48] Tracey Adams, *Online Safety Legislative Reform: A Submission to the Australian Department of Communications and the Arts*, (Brisbane: Yourtown, February 2020), p.3, available at: https://www.communications.gov.au/sites/default/files/submissions/consultation_on_a_new_online_safety_act_-_submission_-_yourtown.pdf

[49] The Carly Ryan Foundation, *Consultation on a new Online Safety Act – Submission,* (Adelaide: The Carly Ryan Foundation, February 2020), p.17, available at: https://www.communications.gov.au/sites/default/files/submissions/consultation_on_a_new_online_safety_act_-_submission_-_the_carly_ryan_foundation.pdf

The EOSA establishes the eSafety Commissioner as an independent statutory office holder that operates with the support of the Australian Communications and Media Authority (ACMA). Both the EOSA and the BSA outline functions and powers afforded to the eSafety Commissioner. The majority of the eSafety Commissioner's functions are expressed in the EOSA, these include education, coordination, grants administration and research functions. The current framework for online safety in Australia also sets out that the eSafety Commissioner has oversight of three regulatory schemes. The EOSA establishes the cyber-bullying scheme addressing serious cyber-bullying of an Australian child, and the image-based abuse scheme addressing the non-consensual sharing of intimate images of all Australians. The BSA sets out the online content scheme, which regulates how illegal and harmful online content is addressed. Under the three schemes, the eSafety Commissioner acts in response to complaints about material, and has some capacity to initiate investigations relating to harmful and illegal online content. The eSafety Commissioner has supported this oversight function by developing cooperative working relationships with social media platforms, content hosts and ISPs in order to effectively remove content hosted in Australia and address harmful online conduct directed at Australians.

The 2018 review concluded that major reform was needed to strengthen the regulatory regime currently outlined in the EOSA and BSA in order to bring it into line with community expectations.

Approach to content hosted outside of Australia

If content is hosted overseas, there is no power in the online content scheme for the eSafety Commissioner to issue take-down notices. The eSafety Commissioner can and frequently does report particularly serious content, such as child abuse material, to international law enforcement for investigation and removal in the host country. If the eSafety Commissioner finds content hosted in Australia to be prohibited content, they would direct the content provider to remove or prevent access to the content. For content hosted overseas found to be prohibited, the URL to the material is added to the eSafety Commissioner's prohibited URLs list.

The eSafety Commissioner's list of prohibited URLs is distributed to PC filter vendors accredited under an Industry Code of Practice. This is more commonly known as the 'family friendly filter' scheme. ISPs offer these filters to their customers. Industry peak body Communications Alliance has noted, however, that many people do not make use of the tools already available to them (such as the family friend filter scheme) to manage their online safety.[50]

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

In April 2019, the eSafety Commissioner was given new powers in the *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019* to issue notices to content service providers and hosting service providers about the presence of abhorrent violent material (AVM). A failure of a service provider to respond to this notice by taking action to remove AVM hosted on their service can lead to criminal prosecution under the Act.

[50] Communications Alliance, *Submission to the Department of Communications and the Arts*, (Sydney: Communications Alliance, February 2020), p.13, available athttps://www.communications.gov.au/sites/default/files/submissions/consultation_on_a_new_online_safety_act_-_submission_-_communications_alliance.pd

ISPs, content service providers (social media services and websites) and hosting service providers are also required to notify the Australian Federal Police (AFP) if they become aware that their service is being used to host abhorrent violent material that is happening in Australia. A failure to do this can also result in criminal prosecution, both for individuals and corporations.

Success of current measures

The current measures for keeping Australians safe online have been effective. The establishment of the eSafety Commissioner as an authoritative voice and strong advocate for safe, respectful online engagement which is trusted by the non-government sector, education bodies, digital industry and the public is a policy success story. The eSafety Commissioner's success in addressing the online safety concerns of Australians includes:

- concluding an average of 11,624 investigations into illegal and harmful content since 2015. Since 1 January 2019, 97 per cent (12,850) of investigations into illegal and harmful content conducted by the eSafety Commissioner were concerned with child abuse material;
- assisting almost 1,800 children and their families to report cyber-bullying and address specific cyber-bullying incidents since July 2015, acting as a safety net for victims where cyber-bullying material is not removed by social media platforms;
- achieving a 100 per cent success rate in seeking the removal of cyber-bullying material from the 'Tier partners' platforms, in some cases as quickly as within 30 minutes from the eSafety Commissioner reaching out to a service;
- responding to over 2,300 reports of image-based abuse since October 2017, having images removed from digital platforms in around 90 per cent of cases;
- issuing 18 abhorrent violent material notices against ten items of content since the Abhorrent Violent Material legislation come into force in April 2019, limiting user access to this content; and
- informally providing assistance to 1,750 adults, mostly women, to respond to online abuse since the eSafety Commissioner's role was expanded to promoting online safety for all Australians in June 2017.

Limitations of current measures

The 2018 Review highlighted a need for improvement to current measures

While the eSafety Commissioner is an effective regulator, the 2018 Review highlighted that improvements to current measures were needed. The review pointed to a need for regulation to reflect the expanded remit of the eSafety Commissioner, apply across the full spectrum of digital devices and address rapidly evolving digital technologies and the growth in overseas hosted harmful material.

The 2018 review recommended:

- replacing the existing legislation with a single Act;
- increasing the expectations on online service providers to be proactive in preventing online harms;

- extending the cyber-bullying scheme to include material directed towards adults; and
- changing the governance arrangements of the eSafety Commissioner to address limitations and deficiencies in the current arrangements.[51]

The eSafety Commissioner's governance arrangements need updating

With the eSafety Commissioner's role expanding to cover the online safety of all Australians, the introduction of the image-based abuse scheme and the administration of numerous programs seeking to promote online safety and protect Australians from online harms, the eSafety Commissioner has outgrown its current governance arrangement. The proposed online safety package would strengthen the financial and operational autonomy of the eSafety Commissioner and address any limitations that exist in the current arrangements.

Harms are occurring on a wider range of online services

Current measures to address online safety for Australians have not kept pace with rapid technological changes and the emergence of new platforms and services. Messaging apps, interactive games and live-streaming services not covered in legislation have given rise to new ways for users to interact and share online content, as well as new ways to contribute to harm done to Australians online. Reforms are needed so that legislation is device and platform neutral, and flexible enough to respond to future changes in technology, industry practices and user habits.

According to the Yellow Social Media Report 2018, 79 per cent of Australians now use social media, representing a 10 per cent increase on social media users in 2017. Further, 99 per cent of young Australians aged 18 to 29 used social media.[52] The same report noted that 45 per cent of social media users in Australia shared an image online, while 59 per cent of Australians access social media every day or most days.[53]

According to Social Media Statistics Australia, in January 2020, Facebook had 16,000,000 active Australian users, while popular messaging and sharing apps also had strong numbers of Australian users. Instagram recorded 9,000,000 monthly active Australian users, WhatsApp recorded 7,000,000 active Australian users and Snapchat recorded 6,400,000 monthly active users.[54]The eSafety Commissioner has recognised the increasing popularity of these apps, and has suggested that risks involved with the use of these apps, include anonymity, the potential for cyber-bullying and the potential for image-based abuse to occur, yet these risks remain inappropriately addressed.[55]

Interactive games are also increasingly being used by Australians. According to the Interactive Games & Entertainment Association (IGEA) Digital Australia Report 2020, two-

[51] "Report of the Statutory Review of the Enhancing Online Safety Act 2015 and the Review of Schedules 5 and 7 to the *Broadcasting Services Act 1992* (Online Content Scheme), pp.42-43.
[52] "Yellow Social Media Report 2018: Part One – Consumers", Yellow, June 2018, p.10 available at: https://www.yellow.com.au/wp-content/uploads/2018/06/Yellow-Social-Media-Report-2018-Consumer.pdf
[53] Ibid.
[54] "Social Media Statistics Australia – January 2020", SocialMediaNews.com.au, February 2020, available at: https://www.socialmedianews.com.au/social-media-statistics-australia-january-2020/
[55] eSafety Commissioner, *Use social media and online chat*, (Sydney: eSafety Commissioner, May 2020), available at: https://www.esafety.gov.au/key-issues/how-to/social-media-online-chat

thirds of Australians played video games.[56] The Report found that games were also being used by 52 per cent of children in school.[57] Harm can occur on these gaming platforms.

According to Kid's Helpline, 50 per cent of online gamers have at some point been bullied within a game, with forms of bullying including name-calling, sexist messaging, exclusion and hate speech.[58] Reforms would capture gaming services within regulation, and appropriately respond to harm occurring within online games.

Online Safety is an increasingly global problem

Current measures to address online safety have not appropriately accounted for the global nature of the internet. While Australian hosted prohibited content can be addressed under the existing online content scheme, most illegal and offensive material is hosted overseas, often in countries with more lenient regulatory environments. These jurisdictions are outside the reach of Australian law enforcement.

Under current arrangements, the eSafety Commissioner does not have extraterritorial powers to address seriously harmful content that is hosted outside of Australia. While the eSafety Commissioner refers overseas hosted illegal content to INHOPE for investigation, and INHOPE works with law enforcement and online service providers in 43 countries to investigate and remove child abuse material. This approach fails to address the full range of illegal material that negatively impacts on Australians, as INHOPE does not address the full range of material that affects online safety, just the worst of the worst.

3. Why is government action needed?

Australians are exposed to harms

Illegal or inappropriate content and conduct is pervasive on the internet. There is a large volume of child abuse and exploitation material, terrorist propaganda, other harmful content and prevalent cyber-bullying online. Australians have been directly impacted by this content and conduct, which has included:

- hundreds, and in some cases thousands, of images and videos linked to the 18,000 reports of child sexual exploitation provided by the Australian Federal Police to the Australian Centre to Counter Child Exploitation (ACCCE) in 2018;[59]
- the proliferation of terrorist materials, such as footage of the Christchurch attacks and the perpetrator's manifesto;
- 3,470 people referred to Kids Helpline from the eSafety Commissioner to gain support in relation to cyber-bullying;[60] and

[56] Jeffrey E. Brand, Jan Jervis, Patrice M. Huggins and Tyler W. Wilson, "Digital Australia 2020", Interactive Games and Entertainment Association, July 2019, p.7 available at: https://igea.net/wp-content/uploads/2019/08/DA20-Report-FINAL-Aug19.pdf
[57] Ibid, p.7.
[58] "Online gaming – is this bullying?", Kids Helpline, 2020, available at: https://kidshelpline.com.au/young-adults/issues/online-gaming-bullying
[59] "Blueprint 2019-2021", Australian Centre to Counter Child Exploitation, July 2018, available at: https://www.accce.gov.au/__data/assets/pdf_file/0008/53576/ACCCEBlueprint.pdf
[60] "Office of the eSafety Commissioner Annual Report 2018-19", p.197.

- requests for assistance from 950 adults to the eSafety Commissioner asking for help dealing with cyber-abuse.[61]

In the absence of strong and consistent industry self-regulation, the proposed reforms are needed to address the exposure of Australians to harm online.

Industry self-regulation is ineffective

Industry has taken action to address online safety concerns on their services, however efforts have proven to be insufficient for managing online harms. Inconsistency across platforms, reactive approaches to the online safety of users and limited reporting requirements have contributed to a failure to protect users from the increased proliferation of harmful content.

Each of the major social media sites, such as Facebook, Twitter and YouTube, have terms of use which govern the relationship with users and others who interact with its site. The Government has worked closely with major social media sites to communicate the expectation that they have:

- terms of use which sufficiently prohibit harmful material; and
- a complaints scheme for reporting harmful material.

Industry has shown a willingness to invest in improving self-regulation and responses to policy-violating or disruptive content. Facebook announced, in September 2019, details of the establishment of an Independent Oversight Board tasked with improving overall transparency efforts over the enforcement of the platforms' policies.[62] The Board includes Australian law professor Nicolas Suzor, a long-time researcher of internet regulation at the Queensland University of Technology.[63] Twitter has also taken steps to strengthen how it handles disruptive behaviours on its platform that negatively impacts or distorts conversation by investing in new tools to address conduct from a behavioural perspective, using behavioural signals to proactively identify violative accounts.[64] Despite these positive steps, platforms and other online service providers do not have sufficiently consistent or comprehensive regulations to address harms online.

Self-regulation is not yet proactive or accountable enough to be sufficient for protecting users from online harms. A report prepared by the French Government highlighted the limitations of self-regulation efforts by digital platforms for addressing online harms. The report noted that digital platforms attempts at self-regulation had been:

- too reactive;
- too inward-looking;
- lacking supervision; and

[61] "Office of the eSafety Commissioner Annual Report 2018-19", p.207.
[62] "Establishing Structure and Governance for an Independent Oversight Board", Facebook, September 2019, available at: https://about.fb.com/news/2019/09/oversight-board-structure/
[63] Ariel Bogle, "An Australian has joined Facebook's oversight board, which will even outweigh Mark Zuckerberg", ABC News, 9 May 2020, available at: https://www.abc.net.au/news/science/2020-05-09/facebook-oversight-board-launches-australian-content-deletion/12225366
[64] Kara Hinesley and Kathleen Reen, *Consultation on a new Online Safety Act Submission – Twitter,* (Sydney: Twitter Australia, February 2020), pp.2-3, available at: https://www.communications.gov.au/sites/default/files/submissions/consultation_on_a_new_online_safety_act_-_submission_-_twitter_australia.pdf

- lacking credibility due to the extreme asymmetry of information on what the platforms are actually doing. [65]

Government intervention is needed to hold industry more accountable for the safety of their products and services. This intervention would operate alongside existing social policy initiatives that address mental health and broader societal issues that contribute to online harms.

Industry is seeking government leadership on some issues

Industry have requested Government leadership on some aspects of online safety reform.

Addressing terrorist and extreme violent material

In the immediate aftermath of the Christchurch Terrorist attacks, major ISPs in Australia voluntarily blocked access to sites known to contain footage of the attacks and the manifesto of the perpetrator. ISPs blocked access to complete domains rather than individual URLs. This meant that much of the offensive material could not be reached. This action, which prevented a great many people being exposed to online harm, also attracted criticism as there was no regulatory requirement to block the sites.

While ISPs have indicated that they stand ready to act to prevent exposure to harmful content, they have called on the Government to provide clear and unambiguous direction, particularly in relation to blocking terrorist and extreme violent material online. ISPs consider that the Australian Government should be responsible for providing direction and legal certainty with respect to what sites to block, how long blocks should be in place and avenues for review. This would provide ISPs with civil immunity from any action or other proceeding for damages as a result of implementing the requested blocks, including on the grounds of 'freedom of expression'.

Freedom of expression

Digital platforms, such as Facebook have suggested a need for Government leadership with respect to ensuring freedom of expression. In their February 2020 report *Charting a Way Forward: Online Content Regulation*, Facebook highlighted the tension between freedom of expression and government attempts to remove harmful online material. The report asked for governments to provide surety that new regulatory frameworks would allow companies to make decisions about online speech in a way that minimises harm but also respects the fundamental right to free expression.[66]

Industry peak body, Communications Alliance, has also expressed concern about the need for government to strike an appropriate balance between the desire to limit the occurrence of the worst types of illegal content and the need for freedom of speech.[67] Industry is seeking leadership by Government on this issue.

Australia needs to keep pace with international developments

[65] "Creating a French Framework to make social media platforms more accountable: Acting in France with a European Vision", Republique Francaise, May 2019, p.12, available at: https://www.numerique.gouv.fr/uploads/Regulation-of-social-networks_Mission-report_ENG.pdf
[66] Monika Bickert, "Charting a Way Forward: Online Content Regulation", Facebook, February 2020, p.1, available at: https://about.fb.com/wp-content/uploads/2020/02/Charting-A-Way-Forward_Online-Content-Regulation-White-Paper-1.pdf
[67] "Submission to the Department of Communications and the Arts", p.11.

The Australian Government has been a world leader in online safety. In 2015, the Government established the world-first Children's eSafety Commissioner to undertake a national leadership role in online safety for Australian children. The Government has also moved swiftly to combat the upload and dissemination of terrorist and violent extremist content, by working with international counterparts in pushing for firm commitments from industry to improve their responses to such content through development of the 2019 agreed proposal for an OECD Voluntary Reporting Protocol. [68] This protocol will provide digital platforms with consistent reporting requirements for addressing terrorist and violent extremist content across OECD member states.[69]

Nevertheless, without the proposed reforms, Australia would fall behind international standards for addressing online harms, as other jurisdictions progress and implement legislative changes that improve how they address online harm. International developments include:

- a proposal for a new statutory 'duty of care' in the United Kingdom that would legally oblige technology firms to protect their users and tackle illegal and harmful activity on their services;[70]
- legislation detailing requirements for digital platforms to remove offensive illegal content within 24 hours in Germany;[71] and
- legislation detailing requirements for digital platforms to remove overtly hateful content within 24 hours in France, and terrorist and child pornography content within one hour of being flagged. [72]

4. Objectives of proposed Government action

The objectives of the proposed reforms are to:

- maintain the elements of the existing framework that are working well, such as the cyber-bullying and image-based abuse schemes;
- address gaps in current regulatory arrangements, particularly where the current schemes are out of date or do not address harms occurring on more recently developed services and platforms;
- establish a more flexible framework that can accommodate new online harms as they emerge;
- hold the perpetrators of harmful online conduct to account for their actions online;
- improve the transparency and accountability of online service providers for the safety of their users and the mitigation of online harms; and

[68] "More Action to Prevent Online Terror", Prime Minister of Australia, August 2019, available at: https://www.pm.gov.au/media/more-action-prevent-online-terror
[69] "More Action to Prevent Online Terror", Prime Minister of Australia, August 2019, available at: https://www.pm.gov.au/media/more-action-prevent-online-terror
[70] "Online Harms White Paper", HM Government, April 2019, p.7, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf
[71] Phillip Ottermann, "Tough new German law puts tech firms and free speech in spotlight", The Guardian, 5 January 2018, available at: https://www.theguardian.com/world/2018/jan/05/tough-new-german-law-puts-tech-firms-and-free-speech-in-spotlight
[72] Hada Gold, Ya Chun Wang and Benjamin Berteau, "French parliament passes law requiring social media companies delete certain content within an hour", CNN Business, 14 May 2020, available at: https://edition.cnn.com/2020/05/13/tech/french-hate-speech-social-media-law/index.html

- enable the eSafety Commissioner to continue to protect Australians online, promote online safety and prevent online harms.

Concerns that have been addressed in the reform proposal

Online safety regulation is a complex challenge

The Government has considered the complex and changing nature of the online environment as well as the impact of new technology and user preferences when developing the proposed reforms. The Government was particularly mindful to consider that:

- many large technology firms that dominate the digital environment are global, and continued engagement with international bodies, such as the Global Internet Forum to Counter Terrorism (GIFCT), may improve Australia's success at improving domestic online safety outcomes;
- social media services, content hosts and technology companies are different, therefore online service providers of varying sizes, maturity and value should not be subject to the same level of regulation;
- the digital landscape is not static and new services and technology will continue to emerge, as will new uses for existing services and technology; and
- the size, impact and reach of services and products will change over time;

There is debate between rights and protections

Online safety reforms are considered necessary to meet the expectations of the Australian community and protect Australians from harm. The reforms have taken into account the scale of harms and the impacts on other rights. For example, content or activity that represents the most risk of real world harm (i.e. national security, extreme violence and child endangerment) are subject to the strictest measures, including removal or prevention of access to that content for Australian users.

The Government continues to be committed to promoting the right to free speech and free expression, which is a hallmark of our democracy. The proposed reforms recognise the importance of highly valued freedoms such as freedom of information, thought and expression and balance the protections of these freedoms with the responsibility to protect vulnerable Australians from harm. In doing this, the reforms would allow vulnerable internet users, including children, to engage equally and safely in the online world.

Ensuring appropriate checks and balances

Importantly, the reforms would retain independent and impartial checks and balances on the exercise of powers provided to the eSafety Commissioner.

Already, a number of decisions made by the eSafety Commissioner around issuing a take-down notice under the current online content scheme can be reviewed by the Administrative Appeals Tribunal. This review mechanism would be maintained with necessary drafting updates to reflect the proposed changes.

Additionally, the Secretary of the Department of Infrastructure, Transport, Regional Development and Communications (formerly Department of Communications and the Arts)

convenes and Chairs a standing Committee on Online Safety of relevant Commonwealth Agency Heads, referred to as the Agency Heads Committee on Online Safety (AHCOS). The Committee promotes and supports the eSafety Commissioner in its role as the primary agency of the Commonwealth's response to online safety. The Committee also identifies opportunities to enhance the effectiveness of Commonwealth policy, regulation and support in relation to online safety. The eSafety Commissioner is a member of AHCOS.

5. What policy options are you considering?

The Government has committed to introducing a new online safety Act to consolidate regulatory arrangements and update them in light of changes in the digital environment. Three options are canvassed below, with option 1 containing no new regulation, option 2 including some new proposals and associated regulation, and option 3 the most comprehensive encompassing all of the new proposals and associated new regulation. As the proposed online safety Act is an election commitment, its development has been included in all three options, albeit in different forms.

Option 1 – A new online safety Act with no regulatory change

Option 1 includes:

- consolidation of existing online safety legislation and mechanisms from the EOSA and Schedules 5 and 7 of the BSA into a new online safety Act, including the image-based abuse scheme, cyber-bullying scheme and online content scheme, with no changes to their operation; and
- reforms to the funding, governance and operations of the eSafety Commissioner.

Option 2 – A new online safety Act with improvements to existing schemes

Option 2 includes:

- the proposals in Option 1;
- improvements to the existing image-based abuse scheme, cyber-bullying scheme and online content scheme; and
- formalisation of content blocking measures for terrorist and extreme violent material online, including improvements to the eSafety Commissioner's response capability; and

Image-based abuse scheme

The definition of image-based abuse under the existing scheme would be expanded to capture images which 'purport to be of a person', and to clearly cover deepfakes and other emerging forms of image-based abuse. Consistent with the other schemes, the time for online services to comply with a take-down notice from the eSafety Commissioner would be reduced from 48 to 24 hours, reflecting how harmful this type of material can be the longer it remains online.

Cyber-bullying scheme

The range of services captured under the existing cyber-bullying scheme would be expanded beyond the largest social media platforms, recognising that bullying and harassment are occurring on multiple platforms, including messaging apps (like WhatsApp), photo-sharing platforms (e.g. Instagram), streaming and video apps (e.g TikTok) and online gaming services (e.g. Fortnite). This would replicate the service coverage in the image-based abuse scheme. Consistent with the other schemes, and consistent with the demonstrated capacity of industry, the time for online services to comply with a take-down notice from the eSafety Commissioner would be reduced from 48 to 24 hours, reflecting how harmful this type of material can be the longer it remains online.

Online content scheme

A revised online content scheme for illegal and harmful online content would allow the eSafety Commissioner to assess content independently of the Classification Board, with problematic content delineated into two categories: Class 1 – seriously harmful content (content that would be unlawful to make available, disseminate, or publish under Commonwealth law such as child abuse material) and Class 2 – harmful content (content that would be classified as X 18+ and MA 15+ under the National Classification Code, including pornography).

The eSafety Commissioner would have the ability to issue take-down notices for Class 1 content (regardless of whether or not it is hosted within Australia), while Class 2 content would be addressed by industry codes, approved by the eSafety Commissioner. The approach taken to issuing take-down notices for Class 1 content hosted overseas is consistent with the eSafety Commissioner's extraterritorial powers to issue notices under the *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019* as well as the existing successful approach to address image-based abuse content.

Industry codes – Provision of an opt-in filtered internet service

Proposed updates to the scheme would include amendments to industry code arrangements. The eSafety Commissioner would work with a range of industry sectors to develop and agree new industry codes that would apply to a wider range of online service providers. The codes would include new requirements for industry to provide the option of an opt-in filtered mobile and broadband service to their customers and to promote the service to consumers.

This industry code requirement would benefit Australians by improving how families with children have access to filtered internet services. As at July 2014, only 4 Australian ISPs had the 'Ladybird Logo' indicating that they agreed to comply with the Communications Alliance's Content Services Codes of Practice, which include a requirement that ISPs provide users with certain information, and the option of obtaining a 'family friendly' content filter.[73] The development of this industry code requirement would expand the availability of filtered internet services to an estimated 1,470,937[74] houses with children and to approximately

[73] "Communications Alliance (CA) Family Friendly ISP Program", Communications Alliance Ltd, July 2014, available at: https://www.commsalliance.com.au/Activities/ispi/ffisp

[74] "Australia: Households with children", *id community demographic resources,* 2016, available at: https://profile.id.com.au/australia/households-with-children

1,174,560 children between the ages of 10 and 16 with mobile broadband coverage (see assumptions in impact analysis section).

Blocking measures for terrorist and extreme violent material

The new Act would give effect to recommendation 5.3 of the *Taskforce to Combat Terrorist and Extreme Violent Material Online* to establish a specific and targeted power for the eSafety Commissioner to direct ISPs to block certain domains containing terrorist or extreme violent material, for time limited periods, in an online crisis event. To provide for a rapid response to online crisis events, it is proposed that the eSafety Commissioner would be provided with the capability to respond to online crisis events 24 hours a day.

Option 3 – A new online safety Act with new and improved schemes

Option 3 includes:

- the proposals in Option 2;
- a new set of basic online safety expectations (BOSE) which articulate the community's expectations of social media services;
- a new 'cyber-abuse scheme' for adults; and
- a new 'ancillary service provider notice' scheme.

Basic online safety expectations

This proposal is for a set of BOSE, set out in a legislative instrument, informed by the Online Safety Charter and the eSafety Commissioner's Safety-by-Design principles, which set out community-led expectations and best practice for industry in preventing online harms. The eSafety Commissioner would have the capacity to require services to report (both publicly and to the regulator) on their actions to comply with the BOSE, and to impose financial penalties for failing to meet these reporting obligations.

The BOSE would initially only apply to social media services, and the eSafety Commissioner would use discretion and a set of criteria in determining which entities would need to report against them. The Minister would also have the power to provide flexibility and relief for smaller platforms.

Cyber-abuse scheme for adults

Recognising the growing harm caused by serious adult cyber-abuse, a new take-down and penalty scheme would be created to encompass cyber-abuse directed at Australian adults. The scheme would establish a higher threshold for what constitutes cyber-abuse than the threshold which applies under the children's cyber-bullying take-down scheme. The services to which the scheme applies, and the 24 hour period to respond to take-down notices, would be consistent with the cyber-bullying and image-based abuse schemes.

Ancillary service provider notice scheme

A new ancillary service provider notice scheme would enable the eSafety Commissioner to collaborate with online services that play a role in disseminating and making available seriously harmful material, but that are not responsible for posting it or enabling users to post

it. Search engines like Google, app stores like those provided by Apple, and video gaming platforms like Steam, all fall into this category. These service providers cannot be held accountable for the content or services they provide access to, but the eSafety Commissioner should be able to require that they delist URLs or cease offering games and apps that themselves host illegal material. These powers would only be used if other avenues for the removal of material have first been tested and not produced an outcome.

6. Impact analysis

Option 1 – A new online safety Act with no regulatory change

Option 1 does not introduce any new regulatory costs on businesses, community organisations or individuals.

Stream 1 / Option 1 annual regulatory costs

Item	Businesses	Community organisations	Individuals	Total change in costs
Total ($ million)	0.000	0.000	0.000	0.000

Option 2 – A new online safety Act with improvements to existing schemes

Option 2 is a compromise between Options 1 and 3, providing some benefits to the community through appropriate amendments to existing schemes, and a lesser regulatory impact on businesses. This option does not introduce any new regulatory costs on community organisations or individuals.

The reduction in the removal timeframe across the existing image-based abuse scheme and cyber-bullying scheme would reduce the potential impact on victims of online harms. During the consultation phase for the development of the new online safety Act, several stakeholders expressed concern that 48 hours was too long to require the removal of image-based abuse and cyber-bullying material following a request from the eSafety Commissioner. They noted that the longer such material is available online, the more harmful it can be for the victim.

Reducing the take-down time to 24 hours would better limit the harm caused by image-based abuse and cyber-bullying, and more closely align with international and industry best practice.
The reduction in time for businesses to respond to a notice would create some additional regulatory costs on businesses, although these are expected to be mostly minor. In practice, the eSafety Commissioner rarely uses formal removal notices, instead opting for a collaborative approach with industry, including informal notices and requests. Most online service providers are already removing content within 24 hours following a formal or informal request from the eSafety Commissioner, thus it is not expected that a reduction in timeframe would create undue burden.

Cyber-bullying and image-based abuse schemes

Recognising that cyber-bullying does not occur exclusively on major social media platforms, expanding the scope of the cyber-bullying scheme to other services would provide victims of serious cyber-bullying on other platforms with additional recourse to deal with complaints.

This would improve health and wellbeing outcomes amongst Australian children and reduce the risk of negative mental health outcomes
The estimated cost to businesses, based on projected business numbers at the conclusion of a 10-year period (see assumptions outlined in **Annex A**) to adhere to changes in the image-based abuse scheme is an average of **$318,000 per annum**. This assumes a projected 18 large businesses (with employment of 200 or more persons), 455 medium businesses (with employment of between 20 and 199 persons) and 3383 small businesses (with employment of between 1 and 19 persons) accessible in Australia after 10 years actioning on average 1 per cent, 0.5 per cent and 0.25 per cent of approximately 849 image-based abuse complaints received by the eSafety Commissioner annually.[75]

The estimated cost to businesses to adhere to changes to the cyber-bullying scheme is **$580,000 per annum**. This assumes a projected 18 large businesses, 440 medium businesses and 3276 small businesses accessible in Australia at the conclusion of a 10-year period (see assumptions outlined in **Annex A**), actioning on average 1 per cent, 0.5 per cent and 0.25 per cent of cyber-bullying complaints respectively (less businesses are affected to account for a decline in the number of businesses with users under the age of 18). This assumption is based on the small number of cyber-bullying complaints that led to formal notices being issued by the eSafety Commissioner in 2018-19.[76]

The regulatory costs associated with these schemes are based on the assumption that the majority of complaints are expected to be managed in the same way that they currently are, which is through the informal collaboration between the eSafety Commissioner and businesses. The new regulatory costs are related to businesses acting on the anticipated small number of formal notices to be issued by the eSafety Commissioner. Further, the calculations assume an average percentage of complaints would be issued to every business as notices; in practice, some businesses, especially large businesses, may receive a higher proportion of notices, while most small businesses would likely receive none.

Online content scheme

Amendments to the online content scheme would better equip the eSafety Commissioner to reduce the availability and spread of illegal and harmful content online, regardless of where it is hosted. A reduction in such content would provide considerable benefit to the community.

Most businesses already have mechanisms in place to respond to requests from the eSafety Commissioner for the removal of illegal and harmful online content. Changes to the online content scheme would require businesses to take down additional content assessed as illegal or harmful by the eSafety Commissioner, and work collaboratively to develop new industry codes.

The estimated cost to businesses to hire new moderation staff and develop new industry codes is **$336,000 per annum** This assumes a projected 18 large businesses, 480 medium businesses and 3562 small businesses accessible in Australia at the conclusion of a 10-year period (see assumptions outlined in **Annex A**), actioning on average 0.1 per cent, 0.05 per cent and 0.025 per cent of sufficiently serious harmful content respectively. The low percentages of serious harmful content that are expected to be referred to businesses for

[75] eSafety Commissioner, *Office of the eSafety Commissioner Annual Report 2018-19*, p.208
[76] eSafety Commissioner, *Office of the eSafety Commissioner Annual Report 2018-19*, p.204

action are based on the eSafety Commissioner's existing practice of actioning most harmful content through other mechanisms including referrals to the Australian Federal Police, filtering software developers, and the international network of online safety hotlines, called INHOPE, for rapid police action and take-down of material in the host country.

Industry codes – Provision of an opt-in filtered internet service

Once agreed through industry codes, the provision of opt-in filtered services to customers will have a regulatory cost for businesses. The estimated cost to business of providing the opt-in filtered service, over a 10-year period is **$3,637,000 per annum**. This cost is based on the estimated number of households and mobile customers that opt-in to the service, as it is anticipated that the service will charge according to the volume of accounts that use it.

Home broadband costings

The cost of the national internet filtering solution is estimated based on a take up rate of 2.5 per cent of all Australian households with children at $55 per year (the minimum cost of commercially-available products). The 2.5 per cent take-up rate is modelled on the take-up of rate of existing industry products, with an increase due to anticipated publicity and promotion of the scheme.

Number of Australian households with children: 1,470,937.[77] Take up rate of 2.5 per cent is: 36,773. The take up (36,773) times the lowest cost filtering solution ($55 per year) is **$2,023,000 per annum**.

Mobile broadband costings

The cost of the mobile broadband filtering solution is estimated based on a take up rate of 2.5 per cent of all Australian children aged ten to sixteen years of age with access to a mobile phone. Children aged younger than ten are likely to have sufficient parental oversight to preclude the use of filters, while children over the age of sixteen are unlikely to require them.

The number of Australian children aged between ten and sixteen years of age was estimated as 1,960,000 in 2016.[78] Factoring in a 1.6 per cent[79] annual population growth rate, the number of Australian children aged ten to sixteen at the conclusion of a 10-year period, starting 2020 is estimated as 2,447,000 persons. As of December 2018, 48 per cent of Australian children had access to a mobile phone,[80] or 1,174,560. A costing based on a 2.5 per cent take up is 29,364. This amounts to a lowest cost filtering solution is **$1,615,000 per annum**.

Requiring industry to provide opt-in filtered broadband and mobile broadband services means that they will lose revenue equivalent to the cost of providing the service. For this reason,

[77] "Australia: Households with children", *id community demographic resources,* 2016, available at: https://profile.id.com.au/australia/households-with-children
[78] "2016 Census QuickStats", *Australian Bureau of Statistics*, October 2017, available at: https://quickstats.censusdata.abs.gov.au/census_services/getproduct/census/2016/quickstat/036
[79] "Australian Demographic Statistics, June 2017", *Australian Bureau of Statistics*, December 2017, available at: https://www.abs.gov.au/ausstats/abs@.nsf/Previousproducts/3101.0Main%20Features2Jun%202017?opendocument&tabname=Summary&prodno=3101.0&issue=Jun%202017&num=&view=
[80] "Kids and mobiles: how Australian children are using mobile phones", Australian Communications and Media Authority, November 2019, available at: https://www.acma.gov.au/publications/2019-11/report/kids-and-mobiles-how-australian-children-are-using-mobile-phones

broadband and mobile broadband providers won't be precluded from recovering the costs of providing the filtered service from users that opt-in. These costs should not exceed the cost of providing the service.

Compliance with this industry code requirement would not change regulatory obligations for community organisations or individuals, there would be no change in costs for these parties.

Regulatory costs of businesses providing an opt-in filtering scheme ($,000)

Item	Businesses	Community organisations	Individuals	Total change in costs
Home broadband	2,023	0.000	0.000	2,022
Mobile broadband	1,615	0.000	0.000	1,615
Total ($ million)	3,638	0.000	0.000	3,638

Formalisation of blocking measures

The formalisation of blocking measures for websites hosting terrorist and extreme violent material, would improve the eSafety Commissioner's ability to reduce the viral spread of such material which has the ability to cause considerable harm and increase the notoriety of perpetrators. Decreased availability of terrorist and extreme violent material may also assist in countering violent extremism by decreasing the exposure of individuals to materials which may radicalise or incite hatred. The proposal would remove ambiguity around this capability for ISPs, and provide legal coverage for ISPs which action blocking notices provided by the Government.

ISPs are already responding to directions from the eSafety Commissioner to block websites hosting terrorist and extreme violent material through existing mechanisms in the Telecommunications Act. Consequently, there are **no additional regulatory costs** to businesses arising from this proposal.

The projected total regulatory cost for businesses arising from Option 2 is measured as **$4,872,000 per annum,** noting that $3,638,000 per annum of the overall cost is associated with the provision of an opt-in filtered internet service, which would only come into effect once agreed through the development of industry codes.

Option 2 annual regulatory costs ($,000)

Item	Businesses	Community organisations	Individuals	Total change in costs
Image-based abuse scheme	318	0	0	318
Cyber-bullying scheme	580	0	0	580
Online content scheme	336	0	0	336
Industry codes –	3,638	0	0	3,638

Provision of an opt-in filtered internet service				
Blocking Measures for Terrorist and Extreme Violent Material	0	0	0	0
Total ($ thousand)	4,872	0	0	4,872

See to **Annex B** for further detail on these calculations from the Regulatory Burden Measure.

Option 3 – A new online safety Act with new and improved schemes

Option 3 provides the most benefit to the community with improvements to existing schemes and the introduction of new schemes to address identified gaps in legislation. Option 3 has the greatest regulatory impact on businesses. This option does not introduce any new regulatory costs on community organisations or individuals.

Basic online safety expectations

The basic online safety expectations (BOSE) would uplift the online safety practices of social media services by providing a clear articulation of the community's expectations. The transparency reporting obligation within the BOSE proposal would create greater transparency of the online safety practices for both government and the community, and encourage uplift through imposing reputational costs for non-compliance.

Compliance with the BOSE would be voluntary, although there is an expectation that social media services would generally seek to uplift their online safety practices to best adhere to the new regulations and avoid potential impacts on company reputation. Social media services would also be expected to produce transparency reports when requested by the eSafety Commissioner, although most large companies are already producing such reports with the appropriately trained staff.

The estimated cost to businesses of uplifting online safety practices and producing transparency reports is **$178,000 per annum**. This assumes a projected 6 large businesses, 60 medium businesses and 50 small businesses accessible in Australia at the conclusion of a 10-year period (see assumptions outlined in **Annex A**) that would each need to produce on average one transparency report per year, and undertake actions to uplift their practices.

Cyber-abuse scheme for adults

The cyber-abuse scheme for adults would provide options for adults who have been the victim of serious online harassment and abuse, and currently have no recourse to formally approach the eSafety Commissioner. The eSafety Commissioner already receives a large number of reports from adults of serious cyber-abuse, although does not possess a formal capability to respond. The scheme would reduce the harm of cyber-abuse by minimising the availability of material, and improve mental health and wellbeing outcomes for adult victims.

The new cyber-abuse scheme for adults would create new regulatory costs for businesses, although some businesses may already have mechanisms in place to respond to complaints of adult cyber-abuse and work collaboratively with the eSafety Commissioner.

The estimated cost to businesses to hire new moderation staff to respond to the cyber-abuse scheme for adults is **$1,076,000 per annum**. This assumes a projected 18 large businesses, 455 medium businesses and 3383 small businesses accessible in Australia at the conclusion of a 10-year period (see assumptions outlined in **Annex A**) actioning on average 1 per cent, 0.5 per cent and 0.25 per cent of cyber-abuse reports respectively.

Ancillary service provider notice scheme

The ancillary service provider notice scheme would provide a reserve power for government in the event that other schemes are ineffective in removing illegal and harmful online content. This would further assist with reducing the community's exposure to illegal and harmful content online and the effects this has on the community's health and wellbeing.

The new ancillary service provider notice scheme is expected to create only a minor regulatory burden on businesses, due to the minimal volume of notices expected. Further, the vast majority of notices would likely be issued to the largest ancillary service providers, including Google, Microsoft and Apple, which already have collaborative relationships with the eSafety Commissioner and delist offending material on a voluntary basis.

The estimated cost to businesses to hire new moderation staff to adhere to the new scheme is **$21,000 per annum**. This assumes a projected 8 large businesses, 20 medium businesses and 26 small businesses accessible in Australia at the conclusion of a 10 year period (see assumptions outlined in **Annex A**) actioning a volume of notices equal to the number expected under the online content scheme. As articulated previously, the low percentages of serious harmful content that are expected to be referred to businesses for action is based on the eSafety Commissioner's existing practice of actioning most harmful content through other mechanisms.

The projected total regulatory cost for businesses arising from Option 3 is measured as **$6,147,000 per annum,** noting that $3,638,000 per annum of the overall cost is associated with the provision of an opt-in filtered internet service, which would only come into effect once agreed through the development of industry codes.

Option 3 annual regulatory costs ($,000)

Item	Businesses	Community organisations	Individuals	Total change in costs
Option 2 costs	4,872	0	0	4,872
Basic online safety expectations	178	0	0	178
Cyber-abuse scheme for adults	1,076	0	0	1,076
Ancillary service provider	21	0	0	21

notice scheme				
Total ($ thousand)	6,147	0	0	6,147

See **Annex B** for further detail on these calculations from the Regulatory Burden Measure.

Regulatory offsets

The Department of Infrastructure, Transport, Regional Development and Communications (DITRDC) will continue work to identify regulatory offsets for the proposed online safety reforms due to the minor net regulatory increase of the proposals. The portfolio's net regulatory objective would be met by the end of the relevant reporting period.

7. What is the best option from those you have considered?

Option 3 – a new online safety Act with new and improved schemes – is considered the best option because it provides the greatest level of protection for Australians from online harms. The proposed measures would have a relatively low regulatory impact, in contrast to the significant benefits that the measures would provide the community and the economy. It is anticipated that the proposed measures would allow the eSafety Commissioner to more effectively address emerging online harms, protect all Australians online and hold perpetrators of harmful online conduct to account. It is also expected that the proposed measures would improve the transparency and accountability of online service providers, including large multinational corporations such as Facebook, Google, Microsoft, Amazon and Twitter. Improved accountability for online service providers would lead to more robust compliance from industry to the government's online safety measures.

Many companies already have staff and processes in place to adhere to new obligations proposed under Option 3; thus, for many of the proposals, the regulatory costs may be nil for certain businesses. Major digital platforms and ISPs already comply with some of the proposed measures, including responding to take-down notices within 24 hours in most cases, complying with the eSafety Commissioner's interim content blocking directions and producing transparency reports.

The reforms would formalise these existing practices and provide certainty to industry. The largest regulatory costs would apply to the major online service providers which account for a large proportion of internet activity, and consequently, a majority of online harms. This includes large multinational corporations which have significant operating revenues.

8. Non-regulatory policy issues

The following proposals form part of the online safety reform package, although are not regulatory so have not been assessed in this Regulation Impact Statement (RIS).

Funding and operations of the eSafety Commissioner

Recognising the expanded remit and duties of the eSafety Commissioner, it is proposed that the eSafety Commissioner would receive additional ongoing funding to allow it to fulfil both existing and proposed functions. To improve the operational autonomy of the eSafety Commissioner, updates to the Commissioner's existing governance arrangements are also proposed.

Online Safety Technology Solutions and Assessment Centre

It is proposed that a pilot for a dedicated Online Safety Technology Solutions Centre (Centre) within the eSafety Commissioner be established in order to build knowledge of, and test, technological and co-regulatory solutions that safeguard Australian children and vulnerable people from online harms. This Centre would support the online safety reform package as a whole by establishing an expert body to research and give online safety technology, co-regulatory, and principles-based solutions to position Government to respond to online safety issues as they arise.

On 5 March 2020, the House of Representatives Standing Committee on Social Policy and Legal Affairs handed down its report into age verification for online wagering and online pornography – *Protecting the age of innocence.*[81] The report recommended that the Government direct and adequately resource the eSafety Commissioner to expeditiously develop and publish a roadmap for the implementation of a regime of mandatory age verification for online pornographic material. It also includes recommendations for complementary measures to allow for age verification to be part of a broader, holistic approach to address risks and harms associated with the exposure of children and young people to online pornography.

It is proposed that the eSafety Commissioner lead in the development of a comprehensive roadmap that would adequately address the complexities of regulating online pornography and that this work be progressed through the Centre. The roadmap would be developed over the next 12-18 months, and provide the Government with a recommendation on whether age verification could be successfully implemented in Australia, and would present options for how this may be progressed.

Following a decision of Government, options for the implementation of a regime for age verification of online pornography in Australia would be subject to further regulatory analysis.

9. Who will you consult about these options and how will you consult them?

DITRDC has undertaken extensive consultation on the proposed reforms and will continue to consult with affected stakeholders throughout the reform process, including during the implementation and review phases.

Completed consultation

The then Hon Paul Fletcher MP, Minister for Communications, Cyber Safety and the Arts announced a ten week public consultation period on proposed reforms to Australia's online safety arrangements on 11 December 2019. The public consultation period ended on 19 February 2020. DITRDC received 86 submissions from a range of stakeholders from digital platforms; non-government organisations; front line service providers; children's groups;

[81] "Protecting the age of innocence", *House of Representatives Standing Committee on Social Policy and Legal Affairs*, March 2020, available at: https://parlinfo.aph.gov.au/parlInfo/download/committees/reportrep/024436/toc_pdf/Protectingtheageofinnocence.pdf;fileType=application%2Fpdf

adult advocacy and legal support services; tertiary education providers; software developers and digital policy advocates; suicide prevention and hate speech advocates; state, territory and local governments; gaming industry and content creators; ISPs; and the Australian public.

Industry Forums

The then Minister for Communications, Cyber Safety and the Arts hosted two industry forums to discuss the proposals, with:

- ISPs and device manufacturers on 31 January 2020; and
- Digital platforms and gaming industry representatives on 17 February 2020.

Civil society engagement

DITRDC undertook extensive stakeholder engagement activities to seek input from civil society stakeholders. DITRDC hosted six roundtable discussions with civil society organisations in Sydney, Canberra and Melbourne. The attendees at these sessions were:

- **Melbourne:** Alannah and Madeline Foundation, Project Rockit, Reality and Risk, Child Wise, Beyond Blue, PartnerSPEAK, InfoXchange, Electronic Frontiers Australia and Domestic Violence Victoria;
- **Canberra:** Foundation for Alcohol Research and Education (FARE), Australian Women Against Violence Alliance and Australian Library and Information Association; and
- **Sydney:** eChildhood, Youth Law Australia, Foundation for Young Australians, Responsible Technology Australia, Australia's National Research Organisation for Women's Safety, Everymind, Women's Safety NSW and Scarlet Alliance.

Meetings or telephone briefings were also arranged with organisations unable to attend roundtables, including Yourtown (Kids Helpline) and the Centre for Inclusive Design.

A total of 58 stakeholders with an interest in online safety were invited to participate in DITRDC's consultation process. Twenty-four organisations attended roundtables or alternative meetings and teleconferences as a part of the consultation process. Information about the consultation period on proposals for a new online safety Act were also provided to the Safe and Supportive School Communities Working Group, the Australian Council of State School Organisations, Australian Parents Council, Catholic School Parents Australia and the Isolated Children's Parents Association.

Engagement with Government

DITRDC alerted all relevant Australian Government departments to the reform proposals and conducted briefings on the proposals with every state and territory government.

Supporting Media

The consultation period was supported by public notices that ran in all major metropolitan newspapers on Saturday 15 February 2020, as well as notices on Facebook, Instagram and Messenger, which ran from 11 February 2020 until 18 February 2020. DITRDC received 28 submissions from private citizens.

Stakeholder views

Basic online safety expectations

The development of basic online safety expectations (BOSE) were commented on by 45 submissions. Civil society groups as well as state and territory governments were particularly supportive of the BOSE concept. Several civil society and adult advocacy and support groups expressed the view that the BOSE, as articulated in the Discussion Paper did not go far enough, and should be mandatory.

Digital platforms and industry groups, whilst broadly supportive of the introduction of the BOSE, and the development of a single reporting framework, expressed concern on its effects on smaller companies. Google noted, in their submission that transparency reporting requirements should be flexible.[82]

Cyber-bullying scheme

Views were received by 28 submissions on a proposal to expand the cyber-bullying scheme for Australian children. The expansion of the scheme was generally well supported. Children's groups and NGOs were pleased with the expanded scope of the scheme as well as the shortened take-down period for cyber-bullying content. Adult advocacy groups, legal support services and tertiary education providers were also broadly supportive of the proposed changes.

Some civil society organisations, including Yourtown,[83] noted that improvements to the scope of the cyber-bullying scheme should occur alongside continued preventative measures by the eSafety Commissioner, including education functions.

Cyber-abuse scheme for adults

A new cyber-abuse scheme for adults was commented on by 32 submissions. The majority of stakeholders supported the introduction of the scheme as well as the higher threshold for what constitutes abuse (compared to the cyber-bullying scheme).

There was some concern expressed by stakeholders, including the Australian Hate Crime Network,[84] that the scope of the scheme did not include discrimination and hostility that may be incited. Further, the Information and Privacy Commission NSW that the higher threshold suggested for cyber-abuse scheme for adults would exclude the deliberate publication of an individual's personal information without their consent.[85]

---

[82] Google Australia Pty Ltd, *Consultation on a new Online Safety Act,* (Sydney: Google Australia Pty Ltd, February 2020), p.2, available at: https://www.communications.gov.au/sites/default/files/submissions/consultation_on_a_new_online_safety_act_-_submission_-_google_australia.pdf

[83] Adams, "Online Safety Legislative Reform: A Submission to the Australian Department of Communications and the Arts", p.11

[84] Nicole L. Asquith, *Submission to the Australian Government's Consultations on a new Online Safety Act*, (Sydney: Australian Hate Crime Network, February 2020), p.15, available at: https://www.communications.gov.au/sites/default/files/submissions/consultation_on_a_new_online_safety_act_-_submission_-_australian_hate_crime_network.pdf

[85] Information and Privacy Commission NSW, *Consultation on a new Online Safety Act,* (Sydney: Information and Privacy Commission NSW, February 2020), p.2, available at: https://www.communications.gov.au/sites/default/files/submissions/consultation_on_a_new_online_safety_act_-_submission_-_information_and_privacy_commission_nsw.pdf

Image-based abuse scheme

Views on a proposed changes to the image-based abuse scheme were received by 23 submission. The changes were largely supported by civil society groups, children's and adult advocacy groups as well as state, territory and local governments. Industry bodies expressed some concern with the proposed reduction in the take-down timeframe for image-based abuse content, with DIGI suggesting that the timeframe was problematic for less resourced companies.[86]

Online content scheme

The updated online content scheme was commented on by 42 submissions. Stakeholders largely agreed that there was a need to modernise and strengthen the online content scheme. This view was particularly pronounced amongst civil society stakeholders.

The development of industry codes that were principles-based were generally welcomed by Communications Alliance.[87]

Blocking measures for terrorist and extreme violent material

The development of blocking measures for terrorist and extreme violent material elicited comments from 18 submissions. The proposal was supported by a majority of industry stakeholders, including major ISPs, the Communications Alliance and most digital platforms that participated in the *Taskforce to Combat Terrorist and Extreme Violent Material Online*. Some adult advocacy groups and legal support services expressed concern that the measures were too broad. Telstra[88] and the Communications Alliance[89] provided suggestions to refine the blocking power, including narrow definitions of key aspects of the legislation to limit its scope to the most harmful content.

Ancillary service provider notice scheme

Views from 21 submissions were received on the proposed new ancillary service provider notice scheme. Predominantly this comprised of civil society, government bodies and education institutions.

Twelve submitters enthusiastically supported the proposal, whilst two were opposed to the new scheme. The remaining seven submissions expressed caution or conditional support, for example, support contingent on the scheme applying to illegal material only.

Future consultation

DITRDC will continue to engage and consult with affected stakeholders throughout the reform process. Some elements of the proposed online safety Act will require further

[86] Bose, "Consultation on a new Online Safety Act – Submission", p.12.
[87] "Submission to the Department of Communications and the Arts", p.9.
[88] Telstra Corporation Limited, *Submission to the Department of Infrastructure, Transport, Regional Development and Communications – Online Safety Legislative Reform Discussion Paper,* (Melbourne: Telstra Corporation Limited, February 2020), p.8, available at: https://www.communications.gov.au/sites/default/files/submissions/consultation_on_a_new_online_safety_act_-_submission_-_telstra_corporation_ltd.pdf
[89] "Submission to the Department of Communications and the Arts", p.14.

consultation at a later stage. For example, DITRDC will consult with digital platforms, civil society groups, governments and other stakeholders on the development of the BOSE to be included in the legislative instrument.

10. How will you implement and evaluate your chosen option?

Implementation

The proposed new online safety Act would come into effect on 1 July 2021. Online service providers would be required to adhere to their legislative obligations from this date.

DITRDC and the eSafety Commissioner would lead a program of extensive stakeholder engagement to allow relevant stakeholders to familiarise themselves with their new regulatory obligations, and the new tools that are available to them. Support would also be provided by DITRDC and the eSafety Commissioner to assist online service providers to understand their new or amended obligations under the new legislation and produce guidance material for this purpose. The public would also be informed of changes to Australia's online safety framework, including the new and amended removal schemes that are available to support victims of online harms.

Evaluation

Following the online safety Act and associated measures coming into effect DITRDC and the eSafety Commissioner would monitor and evaluate the success of the new Act and seek amendments should the measures need to be refined or improved. It is proposed that the Act would be reviewed three years after coming into effect.

The eSafety Commissioner would administer the existing and new schemes, and monitor the volume of complaints and the compliance of online service providers. Information and statistics evaluating the effectiveness of the schemes would be published in the eSafety Commissioner's annual reports.

The progress of social media services in uplifting their online safety practices would be regularly assessed through the transparency reporting obligation in the BOSE proposal. The ongoing research programs of DITRDC and the eSafety Commissioner would also assess improvements in online safety for all online service providers following the implementation of the new Act.

The eSafety Commissioner would continue to be part of, and supported by, the Agency Heads Committee on Online Safety (AHCOS). Further, AHCOS would continue to identify opportunities to enhance the effectiveness of Commonwealth policy, regulation and support in relation to online safety.

Annex A: Regulatory Impact Assumptions

The annual impact of the new online safety Act is costed over a default 10-year duration of the regulation, using projected business numbers at the conclusion of the 10-year period. The regulatory costs in this document are based on the below assumptions.

10-year outlook on the number of businesses impacted

The regulatory burden on businesses is based on an approximation of social media services, ISPs, designated internet services, relevant electronic services and hosting services affected by changes outlined in options 2 and 3. The number of businesses is based on information on small, medium and large businesses from the Australian Bureau of Statistics 'Counts of Australian Businesses, including Entries and Exits June 2015 to June 2019'[90], using 'Data Cube 2: Businesses by Main State by Industry Class by Employment Size Ranges'. Non-employing businesses were not included in the regulation impact statement (RIS), as the size of these businesses would likely preclude them from undertaking activities that would be subject to regulations in a new online safety Act. The ANZSIC codes that are used for reference are:

- 5700 – Internet Publishing and Broadcasting (used to indicate social media services, designated internet services and relevant electronic services).
- 5910 - Internet Service Providers and Web Search Portals (used to indicate internet service providers and designated internet services).
- 5921 – Data Processing and Web Hosting Services (used to indicate hosting services and relevant electronic services).
- 5922 – Electronic Information Storage Services (used to indicate relevant electronic services).

This RIS assumes that the number of small businesses will increase by **6 per cent per annum**, that the number of medium businesses will increase by **12 per cent per annum** and that the number of large businesses impacted by the regulations will increase by **2.5 per cent per annum** over a 10-year period. This approximation of affected businesses after a 10-year period is based on the average increase of small, medium and large businesses in ANZSIC codes 5700, 5910, 5921 and 5922 between the start of the 2018 financial year and the conclusion of the 2019 reporting period.

The total number of small, medium and large businesses is outlined below.

Business size	1-19 Employees (small)	20-199 Employees (medium)	200+ Employees (large)
Projected number of businesses at conclusion of 10-year period	3588 (based on 6 per cent annual increase on 2019 figure of 2004)	500 (based on 12 per cent annual increase on 2019 figure of 161)	26 (based on 2.5 per cent annual increase on 2019 figure of 20)

[90] Australian Bureau of Statistics, *Counts of Australian Businesses, including Entries and Exits, June 2015 to June 2019, Data Cube 2: Businesses by Main State by Industry Class by Employment Size Ranges*, (Canberra, Australian Bureau of Statistics, 20 February 2020), available at: https://www.abs.gov.au/AUSSTATS/abs@.nsf/DetailsPage/8165.0June%202015%20to%20June%202019?OpenDocument

Assumptions of the number of businesses per option

Option 1

Nil regulatory impact

Option 2

Image-based abuse scheme

All small, medium and large businesses except ancillary service providers and websites that may host pornographic material (0.5 per cent of businesses are predicted to be inadvertently hosting pornographic material) are included.

Cyber-bullying scheme

All small, medium and large businesses except ancillary service providers, websites that may host pornographic material (see image-based abuse assumptions for details) and websites that are restricted to children (predicted 3 per cent of relevant businesses) are included.

Online content scheme

All small, medium and large businesses, with the exception of ancillary service providers, may be subject to regulatory impact stemming from this scheme.

Industry codes – Provision of an opt-in filtered internet service

Costs calculated by assessing the fiscal burden on the consumer, which an industry code would transfer onto industry. Regulatory cost for mobile broadband filters assumes that the population of 10 to 16 year olds will increase 1.8 per cent per annum for a 10-year period. There is insufficient data to project a rise or decline in households with families, therefore the household broadband costing remains static. This code represents the most significant regulatory cost for businesses, but would only come into effect once agreed through further consultation.

Blocking measures for terrorist and extreme violent material

Nil regulatory impact.

Option 3

Basic online safety expectations

Assumes that 10 per cent of small internet publishing and broadcasting businesses (ANZSIC code 5700) are social media services subject to the BOSE (increasing 2 per cent per annum), and that 70 per cent of medium internet publishing and broadcasting businesses are social media services subject to the BOSE (increasing 12 per cent per annum).

Six large businesses are presumed to be social media services subject to the BOSE (insufficient evidence to suggest an annual increase).

Cyber-abuse scheme for adults

Accounts for all small, medium and large businesses aside from ancillary service providers, and websites that may host pornographic material (see image-based abuse assumptions for details).

Ancillary service provider notice scheme

Assumes that from a predicted baseline of 26 small ancillary service providers, 20 medium services providers and 8 large businesses in 2020, the number of ancillary service providers will increase by 3 per cent per annum.

Assumptions on the number of complaints

The number of staff, and time, required to action new and improved schemes in the online safety Act assumes current level of complaints to the eSafety Commissioner are maintained. It is not possible to predict a trend in future complaints. It is assumed that any additional burden to businesses to respond to an increase in complaint volumes would be counter-balanced by efficiencies in these businesses, resulting from better processes and new technologies.

Annex B: Regulatory Burden Measure table

Option 2

Business size	# businesses affected	# staff required	# times action performed per year	Time required (hours)	Labour cost	ESTIMATED REGULATORY IMPACT PER YEAR	Notes and assumptions
Image-based abuse scheme							
Small	3383	1	2	0.5	-$ 73.05	-$ 247,000	Assume average 2 notices per business per year (0.25% of total image-based abuse complaints for 2018-19), each report taking an additional 30 minutes to action within 24 hours.
Medium	455	1	4	0.5	-$ 73.05	-$ 66,000	Assume average 4 notices per business per year (0.5% of total image-based abuse complaints for 2018-19), each report taking an additional 30 minutes to action within 24 hours.
Large	18	1	8	0.5	-$ 73.05	-$ 5,000	Assume average 8 notices per business per year (1% of total image-based abuse complaints for 2018-19), each report taking an additional 30 minutes to action within 24 hours.
TOTAL						**-$ 318,000**	
Cyber-bullying scheme							
Small	3276	1	1.25	1.5	-$ 73.05	-$ 449,000	Assume average 1.25 notices per business per year (0.25% of total cyber-bullying complaints for

							2018-19), each report taking 90 minutes to action.
Medium	440	1	2.5	1.5	-$ 73.05	-$ 121,000	Assume average 2.5 notices per business per year (0.5% of total cyber-bullying complaints for 2018-19), each report taking 90 minutes to action.
Large	18	1	5	1.5	-$ 73.05	-$ 10,000	Assume average 5 notices per business per year (1% of total cyber-bullying complaints for 2018-19), each report taking 90 minutes to action.
TOTAL						**-$ 580,000**	
Online content scheme							
Small	3562	1	2	0.5	-$ 73.05	-$ 260,000	Assume average 2 items per business per year (0.025% of total sufficiently serious online content actioned by eSafety Commissioner in 2018-19), each report taking 30 additional minutes to action.
Medium	480	1	4	0.5	-$ 73.05	-$ 70,000	Assume average 4 items per business per year (0.05% of total sufficiently serious online content actioned by eSafety Commissioner in 2018-19), each report taking 30 additional minutes to action.
Large	18	1	8	0.5	-$ 73.05	-$ 35000	Assume average 8 items per business per year (0.1% of total sufficiently serious online content actioned by eSafety

							Commissioner in 2018-19), each report taking 30 additional minutes to action.
TOTAL						**-$ 336,000**	
Industry Codes – Provision of an opt-in filtered internet service							
TOTAL						**-$3,638,000**	
Blocking measures for terrorist and extreme violent material							
Small	0	0	0	0	-$ 73.05	$ -	No regulatory impact on small ISPs.
Medium	0	0	0	0	-$ 73.05	$ -	No regulatory impact on medium ISPs.
Large	0	0	0	0	-$ 73.05	$ -	The 9 identified large ISPs in Australia are already actioning content blocking requests from eSafety Commissioner as current practice, so there is no regulatory impact.
TOTAL						**$ -**	
					TOTAL	**-$4,872,000**	

Option 3

Business size	**# businesses affected**	**# staff required**	**# times action performed per year**	**Time required (hours)**	**Labour cost**	**ESTIMATED REGULATORY IMPACT**	**Notes and assumptions**
Option 2 costs							
TOTAL						**-$ 4,872,000**	
Basic online safety expectations							
Small	50	1	1	7.5	-$ 73.05	-$ 27,000	Assume 1 transparency report per year on average, and

							additional effort to uplift online safety practices, with 1 staff member taking 7.5 hours to produce.
Medium	60	2	1	15	-$ 73.05	-$ 131,000	Assume 1 transparency report per year on average, and additional effort to uplift online safety practices, with 2 staff members taking 15 hours to produce.
Large	6	2	1	22.5	-$ 73.05	-$ 20,000	Assume 1 transparency report per year on average, and additional effort to uplift online safety practices, with 2 staff members taking 22.5 hours to produce.
TOTAL						**-$ 178,000**	
Cyber-abuse scheme for adults							
Small	3383	1	2.25	1.5	-$ 73.05	-$ 834,000	Assume average 2.25 notices per business per year (0.25% of total cyber-abuse reports for 2018-19), each report taking 90 minutes to action.
Medium	455	1	4.5	1.5	-$ 73.05	-$ 224,000	Assume average 4.5 notices per business per year (0.5% of total cyber-abuse reports for 2018-19), each report taking 90 minutes to action.
Large	18	1	9	1.5	-$ 73.05	-$ 18,000	Assume average 9 notices per business per year (1% of total cyber-abuse reports for 2018-19), each report taking 90

							minutes to action.
TOTAL						**-$ 1,076,000**	
Ancillary service provider notice scheme							
Small	26	1	2	1.5	-$ 73.05	-$ 6,000	Assume average 2 notices per business per year (equal to expected number of notices under online content scheme), each report taking 90 minutes to action.
Medium	20	1	4	1.5	-$ 73.05	-$ 9,000	Assume average 4 notices per business per year (equal to expected number of notices under online content scheme), each report taking 90 minutes to action.
Large	8	1	8	1.5	-$ 73.05	-$ 7,000	Assume average 8 notices per business per year (equal to expected number of notices under online content scheme), each report taking 90 minutes to action.
TOTAL						**-$ 21,000**	
					TOTAL	**-$ 6,147,000**	

[1] A small business is a business accessible to Australians with less than 20 employed persons.
[1] A medium business is a business accessible to Australians with between 20 to 199 employed persons.

Statement of Compatibility with Human Rights

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

Online Safety Bill 2021

This Online Safety Bill (the Bill) 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 of the Bill

The purpose of the Bill is to create a new framework for online safety for Australians.

The Bill, together with the Online Safety (Transitional Provisions and Consequential Amendments) Bill 2021, will create a modern, fit for purpose regulatory framework that builds on the strengths of the existing legislative scheme for online safety. In particular, the Bill will:

- retain and replicate provisions in the *Enhancing Online Safety Act 2015* (EOSA) that are working well to protect Australians from online harms, such as the non-consensual sharing of intimate images scheme;
- articulate a core set of new basic online safety expectations to improve and promote online safety for Australians;
- reflect a modernised online content scheme to replace the schemes in Schedules 5 and 7 of the *Broadcasting Services Act 1992* (BSA) to address harmful online content;
- create a new complaints-based, removal notice scheme for cyber-abuse being perpetrated against an Australian adult;
- broaden the cyber-bullying scheme to capture harms occurring on services other than social media;
- reduce the timeframe for service providers to respond to a removal notice from the eSafety Commissioner from 48 to 24 hours;
- bring providers of app distribution services and internet search engine services clearly into the remit of the new online content scheme;
- establish a specific and targeted power for the eSafety Commissioner to request or require internet service providers (ISPs) to disable access to material depicting, promoting, inciting or instructing in abhorrent violent conduct, for time-limited periods in crisis situations, reflecting industry's call for Government leadership on this issue.

Online interactions permeate all aspects of modern life and Australians are using the internet to work, to socialise, to consume entertainment and to engage with government, education, health and financial systems. The Government acknowledges that the internet has brought extraordinary economic, social and educational benefits, which each of us enjoy each day. However, these technologies have also provided avenues for those seeking to do harm.

The Bill strengthens and extends Australia's world-leading online safety framework by adopting and building on the effective elements of the EOSA and Schedules 5 and 7 of the BSA.

This Bill also provides new powers for the eSafety Commissioner to tackle a range of emerging online harms, within a flexible and adaptive framework.

eSafety Commissioner

The Bill establishes the eSafety Commissioner (the Commissioner) and sets out the Commissioner's functions and powers. A key function of the Commissioner is to administer a complaints system for cyber-bullying material targeted at an Australian child; a complaints system for cyber-abuse material targeted at an Australian adult; a complaints and objections system for non-consensual sharing of intimate images and an online content scheme. The Commissioner has the power to investigate complaints and conduct such investigations as the Commissioner sees fit.

Complaints, objections and investigations system

The Bill establishes a complaints systems for:

- cyber-bullying material targeted at an Australian child;
- non-consensual sharing of intimate images;
- cyber-abuse material targeted at an Australian adult; and
- an online content scheme.

Cyber-bullying material targeted at an Australian child

The Bill establishes a system under which persons can make complaints about cyber-bullying material that targets a particular Australian child, and the Commissioner may investigate those complaints. This system builds on the provisions in the EOSA. The Commissioner is able to require the end-user who posted the material to take all reasonable steps to ensure the removal of the material, to refrain from posting further cyber-bullying material for which that person is the target, and/or to apologise to the person for posting the material. This is known as an 'end-user notice'.

The Commissioner has the power to require that the provider of the social media service, relevant electronic service, or designated internet service, remove cyber-bullying material targeted at an Australian child within 24 hours (or such longer period as the Commissioner allows) where the Commissioner receives a complaint that the material was not removed within 48 hours following a complaint made under the service's complaints scheme. The Commissioner can also require a hosting service provider to take all reasonable steps to cease hosting the material.

A person must comply with a requirement under a removal notice from the Commissioner to the extent that the person is capable of doing so. If the social media service, relevant electronic service, designated internet service or hosting service provider fails to do so, they will be subject to a civil penalty.

The Bill contains provisions dealing with the enforcement of these requirements.

Non-consensual sharing of intimate images

Image-based abuse or the sharing of intimate images without consent, is an extremely destructive form of online abuse which can have devastating impacts for victims. The sharing of intimate images without consent is, at times, linked to intimate partner and family violence, with 1 in 4 female victims reporting that perpetrators of image-based abuse had engaged in threatening behaviour after an image was shared.[91]

The Bill establishes a scheme for the removal of such images. The Bill provides that posting, or threatening to post, an intimate image of another person on a social media service, relevant electronic service, or designated internet service without the consent of the person depicted in the image is subject to a civil penalty.

The Commissioner has the power, where certain preconditions are met, to require that the provider of the social media service, relevant electronic service, designated internet service, hosting service or the end-user that posted the image, take all reasonable steps to ensure the removal of the image within 24 hours or such longer period as the Commissioner allows.

Cyber-abuse material targeted at an Australian adult

The Bill establishes a scheme for the removal of cyber-abuse material targeted at an Australian adult that is provided on a social media service, relevant electronic service, or designated internet service.

The Commissioner has the power to require that the provider of a social media service, relevant electronic service, designated internet service, or the end-user that posted the material to remove the cyber-abuse material targeted at an Australian adult within 24 hours, or such longer period as the Commissioner allows, where certain preconditions are met. The Commissioner can also require a hosting service provider to take all reasonable steps to cease hosting the material.

Online content

The Bill establishes a scheme for the removal of class 1 and class 2 material. Complaints may be made to the Commissioner if a person believes that end-users in Australia can access class 1 material or class 2 material, on a particular social media service, relevant electronic service, or designated internet service.

The Commissioner also has the power to order certain actions be taken by app distribution and internet search engine services that play a role in disseminating and making class 1 material available, but that are not directly responsible for the material or their provision. Under the Bill the Commissioner can require app distribution services to cease offering apps that facilitate the posting of class 1 material, and internet search engine services to delete providing links to class 1 material where certain preconditions are met.

[91] Research@eSafety, *Image-Based Abuse National Survey: Summary Report,* (Sydney: eSafety Commissioner, October 2017), p.6, available at: https://www.esafety.gov.au/sites/default/files/2019-07/Image-based-abuse-national-survey-summary-report-2017.pdf

Material relating to abhorrent violent conduct

The Bill establishes a specific and targeted power for the Commissioner to request or require Internet Service Providers (ISPs) to take steps to disable access to material that promotes, incites, depicts or instructs in abhorrent violent conduct, for time limited periods. It is intended to be used in an online crisis event, such as that which occurred after the 2019 terrorist attacks in Christchurch, New Zealand.

To issue a blocking request or notice, the Commissioner must be satisfied that the availability of the material online is likely to cause significant harm to the Australian community. The blocking measures are intended to enable the Commissioner to require ISPs to take rapid, coordinated and decisive action to reduce the viral spread of such material.

Enforcement

The Bill adopts enforcement arrangements set out in the *Regulatory Powers (Standard Provisions) Act 2014* (Regulatory Powers Act), in respect of civil penalties, enforceable undertakings, infringement notices and injunctions for the purposes of the Bill.

Information gathering powers

The Bill establishes the Commissioner's information gathering powers. The Commissioner will have the power to obtain information about the identity of an end-user and the contact details of an end-user from a social media service, relevant electronic service or designated internet service. This power can only be exercised if the Commissioner believes on reasonable grounds that the person has the end-user identity information or contact details, and the information or contact details are relevant to the operation of the Act. An example of where the power might be exercised would be to facilitate the issuing of an end-user notice.

Investigative powers

The Bill establishes the Commissioner's investigative powers. For the purposes of an investigation, the Commissioner has the power to summon a person by written notice to attend before the Commissioner (or a delegate of the Commissioner named in the notice) to produce documents or to answer questions. The Commissioner may also summon a person to provide documents or other information to the Commissioner relevant to the subject matter of an investigation.

Disclosure of information

The Bill enables the Commissioner to disclose information in certain circumstances, including to the Minister, Australian Public Service (APS) employees for the purpose of advising the Minister, Royal Commissions, certain authorities, teachers or school principals, and parents or guardians. This Bill enables the Commissioner to disclose information to teachers or school principals, for example, to assist in the resolution of complaints made under the Act, which may be particularly important in cases of cyber-bullying among school children.

The Bill also deals with associated administrative matters.

Human rights implications

The principal human rights that the Bill engages are:

- the right to freedom of expression primarily contained in Article 19 of the *International Covenant on Civil and Political Rights* (the ICCPR), and also referred to in Articles 12 and 13 of the *Convention on the Rights of the Child* (the CROC) and Article 21 of the *Convention on the Rights of Persons with Disabilities* (the CRPD);
- the prohibition on interference with privacy and attacks on reputation primarily contained in Article 17 of the ICCPR, and also referred to in Article 16 of the CROC, and Article 22 of the CRPD;
- the right to a fair trial and fair hearing rights primarily contained in Article 14 of the ICCPR, and also referred to in Article 40 of the CROC;
- the right to certain minimum guarantees in criminal proceedings, which are contained in Article 14(3), (5), (6) and (7) of the ICCPR;
- the right to protection from exploitation, violence and abuse primarily contained in Article 20(2) of the ICCPR, and also referred to in Article 19(1) of the CROC and Article 16(1) of the CRPD.
- the best interests of the child, contained in Article 3(1) of the CROC.

These rights, and how they are engaged by the Bill, are discussed below.

Freedom of expression

Rights relating to freedom of expression are recognised and protected by Article 19 of the ICCPR and by Articles 12 and 13 of the CROC.

Paragraph 1 of Article 19 of the ICCPR recognises that everyone shall have the right to hold opinions without interference. Paragraph 2 states that everyone shall have the right to freedom of expression. Paragraph 3 of that article recognises that the exercise of this right may be subject to certain restrictions. Paragraph 3 of Article 19 of the ICCPR and paragraph 2 of Article 13 of the CROC limits the types of restrictions that may be imposed, relevantly, to such restrictions as are provided by law and are necessary either for respect of the rights or reputations of others or the protection of national security, public order, health or morals.

The Bill engages the right to freedom of expression to the extent the measures affect individuals rather than corporations:

- It contains provisions that prohibit the non-consensual sharing of intimate images. The prohibition applies if either the person posting the image, or the person depicted in the image, is ordinarily resident in Australia.
- It contains provisions regarding the removal of cyber-abuse material and cyber-bullying material that is provided on a social media service, relevant electronic service and designated internet services (as well as material hosted on hosting services).
- It contains provisions that enable the Commissioner to issue a remedial direction to a person so that they do not contravene the prohibition on the non-consensual sharing of intimate images, or refrain from posting further cyber-bullying material.
- It contains provisions that enable the removal of, or disabling access to, class 1 material on social media services, relevant electronic services and designated

internet services, and provisions regarding the removal or restrictions on access to class 2 material.
- It contains provisions requiring ISPs to take steps to disable access to material that depicts, promotes, incites or instructs in abhorrent violent conduct for time limited periods.

Notwithstanding these restrictions, the Bill is consistent with the freedom of expression, as the restrictions are provided for by law, and are necessary for respect to the rights and reputation of others, or for the protection of national security, public order, health or morals. The measures in the Bill are reasonable and proportionate to achieving the legitimate policy objective of improving and promoting online safety for Australians.

Image-based abuse, cyber-bullying and adult cyber-abuse

Children, young women, Australians of Aboriginal or Torres Strait Islander descent and those who identify as Lesbian, Gay, Bisexual, Transgender, Queer or Intersex (LGBTQI) are particularly vulnerable to online harms. Aboriginal and Torres Strait Islander persons and people identifying as LGBTQI experience online hate speech at more than double the national average.[92] There are many recent examples of ordinary and high profile Australians who have been the target of online bullying and abuse, including associated with domestic violence, which has had serious consequences in a number of cases.

The right to freedom of expression is counter-balanced with the prohibition on interference with a person's right to privacy and attacks on their reputation under Article 17 of the ICCPR and related conventions. People also have the right to protection from exploitation, violence and abuse, as contained in Article 20(2) of the ICCPR and related conventions. Serious harm, including to a person's reputation, can result from the non-consensual sharing of an intimate image, cyber-bullying and adult cyber-abuse. The potential impacts this can have on a person can be long lasting and devastating.

The Australian public recognises the significant harms that can occur online and expect an appropriate regime to be enacted to prevent and minimise these harms. Often the primary goal of victims of these harms is to have the material removed as soon as possible. The powers in the Bill facilitate that goal, and are proportionate and reasonable.

In relation to the image-based abuse scheme, the prohibition on posting an intimate image has been drafted in the least intrusive manner capable of meeting the policy outcome. The prohibition does not prevent the posting of an intimate image if there has been free and express consent provided for the posting of the image. The Bill also includes the concept of an exempt provision which would permit the sharing of an intimate image in particular circumstances. For example, an image could be shared if it is done for the purposes of proceedings in a court or tribunal, if the image is shared for genuine medical or scientific purposes, or an ordinary reasonable person would consider the sharing of the image to be acceptable. These factors ensure that the measures in the Bill are reasonable and proportionate.

[92] eSafety Commissioner, *Online hate speech: Findings from Australia, New Zealand and Europe*, (Sydney: eSafety Commissioner, 2019), p.6, available at: https://www.esafety.gov.au/sites/default/files/2020-01/Hate%20speech-Report.pdf

For cyber-bullying, the Bill engages the right to freedom of expression by requiring the end-user to ensure the removal of cyber-bullying material from a social media service, relevant electronic service or designated internet service following a complaint. The end-user can also be given a notice to refrain from posting cyber-bullying material targeting that child, and to apologise to the child at whom the material was targeted for posting the material.

These provisions are necessary, reasonable and proportionate to respect the rights and reputations of others. The restrictions are the least intrusive necessary to meet the required policy outcome. To be actionable, material must be more than merely offensive or insulting. Importantly, for material to constitute cyber-bullying material under the Bill, it must be such that a reasonable person would conclude that it is likely that the material was intended to have an effect on a particular Australian child, and in addition, it must be such that a reasonable person would conclude that the material would be likely to have the effect of seriously threatening, seriously intimidating, seriously harassing or seriously humiliating the Australian child at whom the material is directed.

In addition, there is scope to narrow the notion of 'cyber-bulling material' that can be actioned under the Bill further by making legislative rules for the purposes of paragraph 6(1)(d). Subclause 6(4) of the Bill also has the effect that material is taken not to be cyber-bullying material if the end-user who posted it was in a position of authority over the child, and posted the material in the lawful exercise of that authority, so long as the posting of the material is reasonable action taken in a reasonable manner.

Having regard to these factors, although the Bill potentially restricts the right to freedom of expression of a person who provides cyber-bullying material on a social media, relevant electronic or designated internet service, it does this in the least restrictive manner that is consistent with achieving the intended policy outcome.

For adult cyber-abuse, the provisions do not prohibit an end-user posting the material, but rather require that material be removed from a service provider's platform following a complaint being made to the provider. The threshold for material to be cyber-abuse targeted at an Australian adult is higher than that for cyber-bullying targeting a child. This is in recognition of the higher levels of resilience expected of Australian adults. For adults, it is only when the material crosses a threshold well beyond reasonable commentary or expression of opinion and into the realm of intentional, serious harm, and being menacing, harassing or offensive, that the Bill provides a mechanism for that material to be taken down from a platform. The provisions, therefore, are reasonable and proportionate to achieve the objective of promoting online safety for Australians.

The right to freedom of expression is further protected under the Bill in that end-users who are subject to notices regarding the removal of cyber-bullying material, adult cyber-abuse material and intimate image material, can appeal those decisions to the Administrative Appeals Tribunal, and have them reviewed by that Tribunal on their merits.

Online content scheme and material that depicts, promotes, incites, or instructs in abhorrent violent conduct

The Bill empowers the Commissioner to require the removal of class 1 or certain types of class 2 material that is provided on a social media service, relevant electronic service or

designated internet service. The Bill also empowers the Commissioner to issue remedial notices to providers so that certain types of class 2 material are subject to access restrictions.

The Bill also provides the Commissioner with a power to prevent search engines and app distribution services from being the conduit to class 1 material. In the event that a search engine can be used by Australian end-users to access class 1 material, the Bill empowers the Commissioner to issue a link deletion notice. Further, the Bill allows the Commissioner to issue app removal notices that will request that online app stores remove apps that facilitate the posting of class 1 material.

The Bill also empowers the Commissioner to require ISPs to disable access to material that depicts, promotes, incites, or instructs in abhorrent violent conduct.

Whilst these measures are directed towards seeking compliance from corporations, it is possible that that the online content scheme affects the rights of individuals generating the content. To the extent that the measures removing these types of material posted by end-users restrict freedom of expression, the restrictions are necessary, reasonable and proportionate for the protection of national security, public order, health or morals and to achieve the legitimate objective of online safety for Australians.

In relation to the blocking power, the Commissioner would need to be satisfied that the availability of the material online is likely to cause significant harm to the Australian community. In considering whether this is the case, the Commissioner is to have regard to the nature of the material (for example, whether it is live-streamed material, particularly high impact material such as a beheading), and the potential for the material to go viral on the internet (i.e. the numbers of end-users who are likely to access the material). The notice power will only be used in these specific circumstances to limit the exposure of Australians to material that depicts, promotes, incites or instructs in abhorrent violent conduct. There are also exemptions for material that relate to a news report or current affairs that is in the public interest, for example, so that the power is sufficiently targeted, and is crafted in a way that is reasonable, proportionate and necessary to achieve the policy objective of online safety for Australians.

The material captured by this blocking power commonly also includes content that contains national, racial or religious hatred seeking to incite violence, especially in relation to radical terrorist or extremist content. Accordingly, the Bill is compatible with and promotes Article 20 of the ICCPR, to the extent it can be said to prohibit advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence.

In relation to the online content scheme, the nature of the material potentially subject to a removal notice is class 1 content, which is seriously harmful content, such as material that depicts cruelty, violent, revolting or abhorrent phenomena in such a way that would offend against standards of morality, decency and propriety generally accepted by reasonable adults (i.e. material that would be refused classification material if classified by the Classification Board). Certain types of class 2 content, such as material that would be X 18+ content, may also be removed by the Commissioner where hosted or provided from Australia. The nature of the material covered by the scheme are such that their unrestricted access would be harmful to Australians, particularly children, and accordingly to the extent that the Bill lawfully restricts freedom of speech through these provisions, those restrictions are reasonable,

proportionate and necessary to achieve the legitimate objective of protecting Australians online.

Finally, clause 233 of the Bill provides that the Bill does not apply to the extent (if any) that it would impinge the constitutional doctrine of implied freedom of political communication. This ensures that the Bill is consistent with the rights to freedom of expression as it relates to political communication.

Protection from unlawful attacks on honour and reputation

Paragraph 1 of Article 16 of the CROC recognises, among other things, the right of a child not to be subjected to unlawful interference with privacy or unlawful attacks on their honour and reputation. Paragraph 2 recognises that children have the right to the protection of the law against such interference or attacks. Article 17 of the ICCPR and Article 22 of the CRPD contain similar rights.

Depending on its particular content, cyber-bullying material, adult cyber-abuse material and intimate images could constitute interference with a person's honour and reputation. By providing remedies for a person who is the target of such material, hence providing the protection of the law against such interferences or attacks, the Bill advances these rights.

Protection from arbitrary or unlawful interference with privacy

Article 17 recognises the right that no one shall be subjected to arbitrary or unlawful interference with their privacy, family, home or correspondence. Article 16 of the CROC and Article 22 of the CRPD contain similar rights.

The articles do not set out the reasons for which the guarantees in it may be limited, however, limitations contained in other articles, for example, those which are necessary in a democratic society in the interests of national security, public order, the protection of the rights or freedoms of others, might be legitimate objectives in appropriate circumstances. In any event, limitations on privacy must be authorised by law and must not be arbitrary.

Image-based abuse, adult cyber-abuse and cyber-bullying

To the extent that the Bill interferes with a person's privacy and correspondence by prohibiting the non-consensual sharing of intimate images, or requiring a person to remove an intimate image, cyber-bullying material or adult cyber-abuse material that has been provided on a social media service, relevant electronic service, or designated internet service, these restrictions are authorised by law, serve a legitimate objective, and are not arbitrary.

The measures in the Bill are fundamentally directed towards protecting the privacy and reputation of vulnerable people. For example, the non-consensual sharing of an intimate image is a serious breach of a person's right to privacy, and often has serious, harmful and reputational consequences for the person depicted in the image. In prohibiting the non-consensual sharing of intimate images, and facilitating quick removal of intimate images through issuing removal notices, the Bill promotes the protection of a person's privacy and reputation. The objectives of harm prevention and minimisation, and protection of privacy and reputation, are legitimate objectives, achieved through reasonable and proportionate means, and are not arbitrary.

Investigations, information gathering and disclosure

To the extent that measures in the Bill would permit the Commissioner to collect personal information, these serve a legitimate objective and are not arbitrary. For example, the Commissioner may receive personal information through the complaints process, or when conducting an investigation into a complaint. Similarly, the information gathering powers in Part 13 allows the Commissioner to obtain information and contact details about the end-user of a social media service, relevant electronic service or designated internet service. The exercise of this power is subject to the Commissioner believing on reasonable grounds that the information or contact details are relevant to the operation of the Act. The collection of this information is necessary to allow for the proper administration of the schemes established by the Bill, and for the proper exercise of the Commissioner's powers, for example, the issuing of end-user notices to end-users.

The Commissioner will be an 'agency' for the purposes of the *Privacy Act 1988* (the Privacy Act), and hence will be bound by the Privacy Act. It is noted that any personal information collected by the Commissioner would be appropriately protected, and dealt with in accordance with the *Privacy Act 1988*.

The purpose of the Bill is to promote the right to privacy, and in relation to the image-based abuse, adult cyber-abuse and cyber-bullying schemes, to protect people from attacks on their reputation and from harm. To the extent that some of the measures in the Bill restrict the right to privacy, these restrictions are provided for by law, serve a legitimate objective, and are not arbitrary.

The Bill expressly authorises by law the disclosures that are permitted by Part 15. Further, the Bill only authorises disclosures in the particular instances dealt with expressly in Part 15. Each of the instances in which disclosure is authorised would, because of the nature of the authorising provisions, be reasonable in the circumstances, as discussed below. Accordingly, the Bill is consistent with the right against arbitrary interferences with privacy.

Under Part 15 of the Bill, disclosure of information by the Commissioner to the Minister responsible for administration of the Bill, and also to the Secretary of the Department and APS employees in the Department who are authorised by the Secretary, for the purpose of advising the Minister, is authorised. Disclosure is also permitted to a member of the staff of the Australian Communications and Media Authority as well as to contractors or consultants engaged to assist the Commissioner.

Disclosure of information under these provisions is not arbitrary, as it is a necessary aspect of the constitutional principle of responsible government. In addition, these provisions authorise disclosures to persons who are similarly bound by the Privacy Act.

Clause 211 of the Bill authorises the Commissioner to disclose information to a Royal Commission (within the meaning of the *Royal Commissions Act 1902*). Royal Commissions are considered to be the highest form of inquiry into substantive matters of public importance, and it is important that the Commissioner not be prevented from participating in any Royal Commission that is relevant to the Commissioner's area of responsibility. However, to ensure

that the right to privacy is protected to the extent possible consistent with the functions and powers of the Royal Commission, subclause 211(2) empowers the Commissioner, by writing, to impose conditions to be complied with in relation to information disclosed under this clause.

Clause 212 of the Bill authorises the Commissioner to disclose information to any of a variety of authorities listed in that clause, if the Commissioner is satisfied that the information will enable or assist the authority to perform or exercise any of its functions or powers. The Commissioner is not the only Commonwealth entity with responsibility for children or for matters relating to cyber-abuse, and others, such as the National Children's Commissioner, would have overlapping areas of responsibility. Further, the Bill is intended to operate alongside a range of State and Territory laws that deal with various aspects of cyber-abuse (clause 234 of the Bill) and is intended not to affect the performance of any State or Territory functions (clause 236 of the Bill). In addition, under the Bill the Commissioner is required to refer material that is of a sufficiently serious nature to warrant referral to law enforcement agencies, including State and Territory police (clause 224 of the Bill). Because of this, clause 212 of the Bill is needed so the Commissioner is able to disclose sufficient information to the authorities listed in that clause. This is so that each of these authorities is able to function to its maximum extent to protect the best interests of affected children and victims of cyber-abuse. To ensure adequate protection of privacy, clause 212 contains a provision which empowers the Commissioner, by writing, to impose conditions to be complied with in relation to information disclosed under this clause. This may include, for example, conditions that prevent further disclosure to third parties.

Clauses 213 and 214 are similar provisions, which provide that the Commissioner is able to disclose information to a teacher or school principal, or to a parent or guardian, if the Commissioner is satisfied that the information will assist in the resolution of a complaint under the Bill. Resolution of a complaint by teachers or principals, or parents or guardians, has advantages over resolution through the more formal regulatory channels available under the Bill, particularly dealing with instances of cyber-bullying that might be of a less serious nature. These clauses facilitate resolution of complaints in such a manner. By facilitating resolution of complaints outside of the more formal channels, the Bill is also intending to minimise the adverse impacts of its provisions on the right to freedom of expression, discussed above. Clauses 212 and 213 contain provisions to empower the Commissioner, by writing, to impose conditions to be complied with in relation to information disclosed under these clauses.

Other provisions of Part 15 of the Bill are consistent with the right to privacy. Clause 215 permits disclosure of information relating to the affairs of a person, so long as that person has consented to that disclosure, and clause 216 authorises the disclosure of information that is already publicly available. Clause 217 authorises the disclosure of summaries and statistics, but these are only authorised if they are summaries of, or statistics prepared from, 'de-identified' information. The term 'de-identified' is defined in clause 5 as information that is no longer about an identifiable individual, or an individual who is reasonably identifiable. This ensures that the right to privacy is preserved when information is disclosed under this provision.

The right to a fair trial and fair hearing rights; the right to minimum guarantees in criminal proceedings

Triggering of civil penalty provisions in the Regulatory Powers Act

Article 14 of the ICCPR recognises certain minimum guarantees in criminal proceedings. A penalty may be 'criminal' for the purposes of the ICCPR even if it is 'civil' under Australian domestic law. Accordingly, it needs to be considered whether the triggering of provisions in the Regulatory Powers Act by the Bill would engage criminal process rights under the ICCPR.

Triggering the civil penalty provisions of the Regulatory Powers Act could engage criminal process rights if the imposition of civil penalties is classified as 'criminal' under international human rights law. Article 14 of the ICCPR requires that, in the determination of criminal charges, everyone shall be entitled to a fair and public hearing by a competent, independent and impartial tribunal established by law. Various other rights are provided for persons charged with criminal offences.

Determining whether penalties could be considered to be criminal under international human rights law requires consideration of the classification of the penalty provisions under Australian domestic law, the nature and purpose of the penalties, and the severity of the penalties.

The penalty provisions in the Bill are expressly classified as civil penalties. The purpose of most of these penalties is to encourage compliance with a removal notice or remedial direction given to a person. The civil penalty provisions in the Bill do not impose criminal liability, and do not lead to the creation of a criminal record. The penalties would only apply to those who have contravened the provision, rather than the public in general.

The amount of 500 penalty units applies to a contravention of a civil penalty provision for failure to comply with removal notices under the schemes. This amount reflects the significant harm and distress that can be caused to a person from the failure to remove material subject to the removal notices. It also reflects that the failure to comply with a removal notice or a remedial direction can cause significant distress and harm in itself.

It is noted that under the Regulatory Powers Act, when determining the amount of the penalty to be imposed, a court is required to consider the nature and extent of the contravention, the loss and damage suffered because of the contravention, the circumstances in which the contravention took place, and whether the person has been found by a court to have engaged in similar conduct in the past. This provides the court with a discretion, in light of the circumstances of the case, to impose an appropriate penalty of up to 500 penalty units if the person is found to be in contravention of this provision. That is, a court could decide not to impose the full 500 penalty units in relation to a contravention. The penalty provisions do not carry the possibility of imprisonment.

These factors all suggest that the civil penalties imposed by the Bill are civil rather criminal in nature. Accordingly, the criminal process rights provided for by Article 14 of the ICCPR are not engaged by the Bill relating to civil penalty orders.

Triggering infringement notice provisions in the Regulatory Powers Act

The Bill also triggers the infringement notice provisions contained in Part 5 of the Regulatory Powers Act in relation to periodic and non-periodic reporting, failure to comply with removal notices, failure to adhere to remedial directions and non-compliance with industry codes and directions. There are no criminal consequences associated with an infringement notice for a contravention of a civil penalty provision. For example, an infringement notice does not carry the possibility of imprisonment if the person does not pay the penalty specified in the notice. There is a requirement under the Regulatory Powers Act that an infringement notice state that the person may choose not to pay the penalty and notify them that, if they do so, proceedings seeking a civil penalty order may be sought against them in a court. The maximum penalty that an infringement notice can impose on a natural person is 12 penalty units, and the person can always request the relevant chief executive to withdraw the infringement notice.

These factors all suggest that the infringement notice provisions triggered by this Bill are civil rather than criminal in nature. Accordingly, the criminal process rights provided for by Article 14 of the ICCPR are not engaged by the Bill in relation to the issuing of infringement notices for breach of the civil penalty provisions. Further, as the person may elect to have the matter heard by a court, rather than pay the amount in the infringement notice, the right to a fair hearing in civil matters provided for by Article 14(1) of the ICCPR is engaged, but not limited (for the reasons discussed above).

Triggering enforceable undertaking provisions in the Regulatory Powers Act

The Bill also triggers the enforceable undertaking provisions in Part 6 of the Regulatory Powers Act, which will allow the Commissioner to accept and enforce undertakings relating to compliance with the prohibition on the non-consensual sharing of intimate images, removal notices or a remedial direction. Further, if the Commissioner is satisfied the person has breached the undertaking, the Commissioner may apply to a relevant court for an order relating to the undertaking.

Accordingly, the triggering of these provisions engages the right to a fair and public hearing in civil proceedings. As an order enforcing an undertaking can only be made by the Federal Circuit Court of Australia, or the Federal Court of Australia, both of which are competent, independent and impartial courts established by law, this right is engaged but not limited (for the reasons discussed above).

Triggering injunction provisions in the Regulatory Powers Act

The Bill also triggers the injunction provisions in Part 7 of the Regulatory Powers Act, which will enable the Commissioner to apply to a relevant court for an injunction restraining the person from engaging in conduct, or requiring the person to do a particular thing. In particular, the Commissioner would be able to seek an injunction in relation to a threat to contravene the prohibition on the non-consensual sharing of intimate images, or a failure to comply with a removal notice or remedial direction.

Triggering the injunction provisions of the Regulatory Powers Act engages the right to a fair and public hearing in civil proceedings. As an injunction can only be issued by the Federal Circuit Court of Australia or the Federal Court of Australia, both of which are competent, independent and impartial courts established by law, this right is engaged but not limited (for the reasons discussed above).

The right to protection from exploitation, violence and abuse

The right to protection from exploitation, violence and abuse is primarily contained in Article 20(2) of the ICCPR and other related conventions. The ICCPR and related conventions requires Australia to take measures to protect persons from exploitation, violence and abuse.

This right is engaged as the image-based abuse scheme, adult cyber-abuse scheme and cyber-bullying schemes in the Bill are directed to protecting people from serious harm that can result from the non-consensual sharing of an intimate image, or abusive or bullying behaviour. Exploitative acts can be involved in the non-consensual sharing of intimate images that often causes significant harm and distress to the person depicted in the image. Similarly, victims of cyber-abuse can be the subject of volumetric attacks (or 'pile ons') across multiple platforms, where a person is named in, tagged, or linked to an abusive post, which others like, share, re-post with additional commentary, or link to via other services. The volume of material can proliferate rapidly across platforms, resulting in hundreds or thousands of related posts focused on a single individual. In severe cases, these attacks can lead to the 'doxing' of personal information and in-person violence.

The purpose of the Bill is to deter people from engaging in this behaviour, and to provide the Commissioner with an appropriate enforcement mechanism to address it, through conferring powers on the Commissioner to issue removal notices, remedial directions and civil penalties for non-compliance. The Bill promotes the right to protection from exploitation, violence and abuse as it provides mechanisms for persons to complain and have harmful content targeted against them removed.

Accordingly, the Bill is consistent with the right to protection from exploitation, violence and abuse, as the measures contained in the Bill are directed towards the protection of persons from exploitation, violence and abuse.

Best interests of the child

Article 3(1) of the CROC provides that in all actions concerning children, the best interests of the child shall be a primary consideration. The principle requires legislative, administrative and judicial bodies to take active measures to protect children's rights, promote their wellbeing and consider how children's rights and interests are or will be affected by their decisions and actions.

The Bill supports the best interests of the child by providing mechanisms so that children are protected from seriously harmful content, as well as cyber-bullying material and the non-consensual sharing of intimate images.

Conclusion

This Bill 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*.

The measures in the Bill do not limit the right to a fair and public hearing in civil proceedings, to the extent the measures engage that right.

The measures in the Bill promote the right to protection from exploitation, violence and abuse, the right to protection from unlawful attacks on honour and reputation and the best interests of the child.

To the extent to which the measures in the Bill may engage the right to freedom of expression, the right to privacy and the right to certain minimum guarantees in criminal proceedings, any limitation is reasonable, necessary and proportionate to the goal of promoting and improving online safety for Australians.

NOTES ON CLAUSES

PART 1 – PRELIMINARY

Part 1 of the Online Safety Bill (the Bill) deals with preliminary matters including objects, commencement and definitions.

Clause 1 – Short Title

Clause 1 provides that the Bill, when enacted, may be cited as the *Online Safety Act 2021*.

This title reflects that this Bill will provide a comprehensive regulatory framework for online safety for Australians.

Clause 2 – Commencement

Clause 2 provides for the commencement of the Bill.

Subclause 2(1) provides that the provisions listed in column 1 of the table, currently the whole of this Act, commences upon a single date to be fixed by Proclamation, and includes a standard provision providing for automatic commencement of the provisions referred to in column 2 of the table within six months of the Act receiving the Royal Assent if they have not commenced sooner by Proclamation under that subclause.

Subclause 2(2) is a standard provision which provides that information inserted in Column 3 of subclause 2(1) is not a part of the Act. Subclause 2(2) allows for the date of commencement of subclauses under subclause 2(1) to be listed in Column 3 in any published version of the Act.

Clause 3 – Objects of the Act

Clause 3 provides that the objects of the Act are to improve and promote online safety for Australians.

Clause 4 – Simplified outline of this Act

Clause 4 is a simplified outline of the Bill. This simplified outline is included to assist readers to understand the substantive provisions of the Bill. However, the outline is not intended to be comprehensive. It is intended that readers should rely on the substantive provisions of the Bill.

Clause 5 – Definitions

Clause 5 defines terms used in the Bill. The definitions of many of these terms are self-explanatory. Definitions of particular note are as follows:

app distribution service is intended to include services that meet the definition and are available on a range of receptive communications devices including, but not limited to, computers, tablets, gaming devices, digital televisions, electronic books and mobile phones.

basic online safety expectations (see clause 45)

class 1 material (see clause 106)

class 2 material (see clause 107)

cyber-abuse material targeted at an Australian adult (see clause 7)

cyber-bullying material targeted at an Australian child (see clause 6)

designated internet service (see clause 14)

data storage device is a device used to host stored material or content, whether that content can be accessed or distributed by a carriage service while on that device or not. As an example, a Universal Serial Bus (USB) device that is used to store content separately from a receptive communication device (such as a computer or mobile phone) is included within this definition, as is internet-based (cloud) storage, as is hardware such as a memory card or server.

A device that only stores the material on a highly transitory basis, such as during a transmission relay process, is not included within this definition. An example of this may be a router, which may momentarily store material while buffering.

electronic service is used to refer to media-rich audio-visual services delivered over new platforms using a carriage service. This includes, but is not limited to, services delivered by cabled or wireless internet, mobile telecommunications services, and any other means of delivery that uses guided and/or unguided electromagnetic energy, to a range of receptive communications devices such as computers, tablets, gaming devices, digital televisions, electronic books and mobile phones.

Mobile internet access, mobile and online games, retransmitted broadcasting content, mobile chat rooms and proprietary network content portals are some examples of the kinds of services available over mobile phones and other communications devices.

Electronic services do not include a broadcasting service or a datacasting service, which are to remain separately regulated under the BSA.

hosting service (see clause 17)

material is intended to be read as broadly as possible. It includes any content in any form, or in any other combination of forms.

on-demand program service (see clause 18)

posted (see clause 11)

provided (see clause 10)

relevant electronic service (see clause 13A)

serious harm includes both physical harm and harm to mental health but is not intended to include harm from being subjected to any force or impact that is within the limits of what is acceptable as incidental to social interaction or to life in the community. It is not intended to include mere ordinary emotional reactions. Serious harm is defined to mean temporary or permanent harm. This term is used in the definition of cyber-abuse material targeted at an Australian adult in clause 7 of the Bill.

serious harm to a person's mental health includes serious psychological harm and serious distress. It is not intended to include harm from being subjected to impact that is within the limits of what is acceptable as incidental to social interaction or to life in the community. It is not intended to include mere ordinary emotional reactions.

social media service (see clause 13)

stored material means material kept on a data storage device. It is not intended to capture any storage of material on a highly transitory basis as an integral function of the technology used in its transmission. This term is used in the definition of a hosting service in clause 17 of the Bill.

Other definitional and interpretive provisions are contained in clauses 6, 7, 8, 9, 10, 11, 12, 13, 13A, 14, 15, 16, 17, 18, 19, 20, 21, 45, 86, 106, 107, 108, 151, 238, and 239.

Clause 6 – Cyber-bullying material targeted at an Australian child

This clause sets out the criteria for determining whether material submitted as part of a complaint to the Commissioner under clause 30 is 'cyber-bullying material targeted at an Australian child'.

Paragraph 6(1)(a) requires that the material be provided on a social media service, relevant electronic service or designated internet service.

Subclause 6(1) applies an objective test in paragraph (b) to determine whether an ordinary reasonable person would conclude that it is likely that the material was intended to have an effect on a particular Australian child, and that the material would be likely to have the effect on the Australian child of seriously threatening, seriously intimidating, seriously harassing or seriously humiliating the Australian child. For the purposes of subclause 6(1), 'threatening', 'intimidating', 'harassing' and 'humiliating' are intended to have their ordinary meaning.

If all the conditions in paragraphs (a) to (c) are satisfied, then subclause 6(1) provides that the material in question is 'cyber-bullying material targeted at the Australian child' and the Australian child is the target of the material. The requirement that the material 'was intended to have an effect on the Australian child' in subparagraph 6(1)(b)(i), is designed to exclude material of a general nature, such as material targeted at a broad class of people.

Paragraph 6(1)(c) enables other conditions to be included in the test of 'cyber-bullying material targeted at an Australian child' by the legislative rules (see clause 240) should it become apparent during the course of administering the legislation that further conditions should be specified.

Subclause 6(2) provides that an effect mentioned in subclause 6(1) may be a direct result of material being accessed by, or delivered to, the Australian child or an indirect result of the material being accessed by, or delivered to, one or more other persons. This subclause is intended to capture indirect effects of cyber-bullying material which are not directly accessed by the Australian child, but which still have an effect on the child, for example, by material being accessed by, or delivered to, other children in the child's class at school.

Subclause 6(3) limits the effect of subclause 6(1) to the extent that subclause 6(4) applies.

Subclause 6(4) provides an exception to subclause 6(1) for material posted by persons who are in a position of authority over an Australian child, so as not to interfere with reasonable action taken in a reasonable manner by authority figures. Reasonable action taken in a reasonable manner by authority figures such as parents, teachers and employers could include matters such as notifying the child by email of exam results or dismissal from employment. Such matters should not be treated as cyber-bullying.

Clause 7 – Cyber-abuse material targeted at an Australian adult

This clause sets out the criteria for determining whether material submitted as part of a complaint to the Commissioner under clause 36 is cyber-abuse material targeted at an Australian adult.

There are 4 limbs that must be satisfied before material meets the test for cyber-abuse material targeted at an Australian adult. These are set out in subclause 7(1):

- the material has been provided on a social media service, relevant electronic service or a designated internet service (paragraph (a));
  applying an objective test, determining whether an ordinary reasonable person would conclude that it is likely that the material was intended to have an effect of causing serious harm to a particular adult (paragraph (b));
- applying an objective test, determining whether an ordinary reasonable person in the position of the Australian adult would regard the material as being, in all the circumstances, menacing, harassing or offensive (paragraph (c)); and
- such other conditions (if any) are met, as set out in the legislative rules (paragraph (d)).

Subclause 7(1) applies an objective test in paragraph (b) to determine whether an ordinary reasonable person would conclude that it is likely that the material was intended to have an effect of causing serious harm to a particular Australian adult. ***Serious harm*** is defined in clause 5 as meaning serious physical harm or serious harm to a person's mental health, whether temporary or permanent. ***Serious harm to a person's mental health*** is also defined as including serious harm or serious distress. It is not intended that mere ordinary emotional reactions or distress within the limits of what is acceptable as incidental to social interaction or to life in the community be captured by this definition.

The requirement that it is likely that the material was intended to have an effect of causing serious harm to 'a particular Australian adult' in paragraph (b), is designed to exclude material of a general nature, such as material targeted at a broad class of people.

Subclause 7(1) also applies an objective test in paragraph (c) to determine whether an ordinary reasonable person in the position of the Australian adult would regard the material as

being, in all of the circumstances, menacing, harassing or offensive. In other words, it is intended that, whilst the circumstances of a particular adult would be relevant to how that person would regard the material, it would be how an ordinary reasonable person in those circumstances would regard the material that is relevant.

The test to determine if material is offensive is in clause 8 below.

In determining whether material is 'cyber-abuse material targeted at an Australian adult', the Commissioner may consider the context in which the abuse occurs, for example whether a person has been targeted because of their cultural background, gender, sexual orientation, disability, mental health condition or family or domestic violence situations. The intention is also for the Commissioner to consider the ordinary meaning of 'menacing' and 'harassing'.

The definition is not intended to capture 'reputational harm' caused by defamatory material, for example negative online reviews of businesses. However, defamatory material may be determined to be 'cyber-abuse material targeted at an Australian adult' where an intent to cause serious mental or physical harm to a person can be established.

Paragraph 7(1)(d) enables other conditions to be included in the test of 'cyber-abuse material targeted at an Australian adult' by the legislative rules (see clause 240) should it become apparent during the course of administering the legislation that further conditions should be specified.

If all the conditions in paragraphs (a) to (d) are satisfied, then subclause 7(1) provides that the material in question is 'cyber-abuse material targeted at an Australian adult' and the Australian adult is the target of the material.

Subclause 7(2) provides that an effect mentioned in paragraph 7(1)(b) may be a direct result of material being accessed by, or delivered to, the Australian adult or an indirect result of the material being accessed by, or delivered to, one or more other persons. This subclause is intended to capture indirect effects of cyber-abuse material which are not directly accessed by the Australian adult, but which still have an effect of causing serious harm to an Australian adult.

Clause 8 – Determining whether material is offensive

Clause 8 provides for the matters to be taken into account in deciding for the purposes of the Act whether an ordinary reasonable person in the position of the Australian adult would regard particular material as being, in all the circumstances, offensive. This is an objective test. Subclause 8(1) provides that the matters to be taken into account include the standards of morality, decency and propriety generally accepted by reasonable adults, the literary, artistic or educational merits (if any) of the material, and the general character of the material (including whether it is of a medical, legal or scientific character).

Paragraphs 8(2)(a) and 8(2)(b) provide for circumstances where the material is private sexual material and is provided on a social media service, a relevant electronic service or a designated internet service. Subclause 8(2) provides that when applying the objective test of whether an ordinary reasonable person in the position of a particular Australian adult would regard the material as being offensive, the consent of the subjects to have the private sexual

material provided on the service must also be regarded. Subclause 8(3) provides that subclause 8(2) does not limit subclause 8(1).

Clause 9 – Material that depicts abhorrent violent conduct

Clause 9 defines the material that depicts abhorrent violent conduct for the purposes of the Bill.

Clause 9 provides that audio material, visual material or audio-visual material that records or streams abhorrent violent conduct is to be considered 'material that depicts abhorrent violent conduct.' 'Abhorrent violent conduct' is a defined term for the purposes of the Bill (see clause 5).

Subclause 9(2) provides that it does not matter whether the material has been altered. The intention is that material that ordinarily meets the definition of 'material that depicts abhorrent violent conduct' would remain as such, even if a person has edited the material in some way.

The intention of subclause 9(2) is to capture altered forms of such material within the operation of Part 8. A practical example is the video made by the perpetrator of the 2019 Christchurch terror attacks. Both the full, unedited stream created by the perpetrator of the Christchurch attacks is material that depicts abhorrent violent conduct, as are any versions of that material that are edited in some way.

Clause 10 – When material is provided on a social media service, relevant electronic service or designated internet service

Clause 10 provides for the conditions that must be met for material to be considered as having been ***provided*** on a social media service, relevant electronic service or designated internet service. These condition are that the material is accessible or delivered to an end-user of the service.

Clause 11 – When material is posted by an end-user of a social media service, relevant electronic service or designated internet service

Clause 11 provides for the conditions that must be met for material to be considered as having been ***posted*** on a social media service, relevant electronic service or designated internet service. These conditions are that the material is accessible or delivered to an end-user of the service. The purpose of this clause is to capture material posted on a service, as well as cases where an end-user posts a hashtag, or link, for example, which causes the material to be accessible to another end-user of the service.

Clause 12 – When material is removed from a social media service, relevant electronic service or designated internet service

Clause 12 provides for the conditions that must be met for material to be considered as having been ***removed*** from a social media service, relevant electronic service or designated internet service.

Clause 12 stipulates that material is removed from a social media service or relevant electronic service if the material is neither accessible to, nor delivered to, any of the end-users in Australia using the service.

For this purpose, it is intended that if specifically identified material is removed, the material is taken to be removed even if a copy of the same material, within the control of another end-user, is accessible to, or delivered to, one or more other end-users using the service. It would not be reasonable to expect social media services to remove material that is not specifically identified to them.

Clause 13 – Social media service

Clause 13 defines the term ***social media service*** for the purposes of the Bill.

Subclause 13(1) provides that a 'social media service' is an electronic service that satisfies the conditions listed in paragraph (a), or is specified in the legislative rules, but does not include an exempt service as defined by subclause 13(4).

The term 'electronic service' is defined in clause 5 of the Bill as a service that allows end-users to access material using a carriage service or a service that delivers material by means of a carriage service. 'Carriage service' is defined in the *Telecommunications Act 1997* to mean a service for carrying communications by means of guided or unguided electromagnetic energy. The definition of electronic service specifically excludes broadcasting and datacasting services as defined in the *Broadcasting Services Act 1992* (BSA).

A social media service does not need to use the internet to be a social media service but can use another form of carriage service.

Subparagraph 13(1)(a)(i) provides that to be a social media service, the sole or primary purpose of the service must be to enable online social interaction between 2 or more end-users. It is not intended that subparagraph (a)(i) would capture online games that have chat functionality (where the primary purpose of such a service would be to play the game).

Subparagraphs 13(1)(a)(ii), (iii) and (iv) provide that to be a social media service, the electronic service must allow end-users to link to, or interact with, some or all of the other end-users, allow end-users to post material on the service and satisfy any other conditions as are set out in legislative rules (see clause 240).

Subclause 13(1) includes a note making it clear that online social interaction does not include online business interaction. For example, it is not intended that subparagraph (a)(i) would capture online feedback facilities established by businesses for the purposes of dealing with their customers.

Subclause 13(2) clarifies that, in the 'sole or primary purpose of the service' test in subparagraph 13(1)(a)(i), online social interaction includes online interaction that enables end-users to share material for social purposes (which does not include business purposes as clarified by the note).

Subclause 13(3) clarifies that, in determining whether the 'sole or primary purpose of the service' test in subparagraph 13(1)(a)(i) is satisfied, the following purposes are to be disregarded:

- the provision of advertising material on the service;

- the generation of revenue from the provision of advertising material on the service.

Subclause 13(3) will provide that services that would otherwise meet at least one of the sets of conditions in subclause 13(1) do not fall outside of the 'social media service' definition on the basis of an argument that the sole or primary purpose of such a service is to sell advertising or generate revenue from advertising sales.

Exempt services

Subclause 13(4) provides for exempt services.

A service is exempt from being a 'social media service' for the purposes of the Bill if:

- none of the material on the service is accessible to, or delivered to, one or more end-users in Australia (paragraph 13(4)(a)). This is intended to limit the jurisdiction of the Bill so that social media services that are not accessible to end-users in Australia would not be subject to the Bill; or
- the service is specified in the legislative rules (paragraph 13(4)(b)). This is to build in flexibility for certain circumstances where it may be appropriate for a particular social media service to be exempt.

Clause 13A – Relevant electronic service

Clause 13A inserts a definition of ***relevant electronic service*** that means any of the electronic services listed in the definition including: a service that enables end-users to communicate with other end-users by email; instant messaging; short message service (SMS); multimedia message service (MMS); or a chat service or a service that enables end-users to play online games with other end-users.

The definition also includes any electronic service that is specified in legislative rules made by the Minister.

Subclause 13A(2) inserts a definition of an ***exempt service*** to mean services where none of the material on the service is accessible to, or delivered to, one or more end-users in Australia. This is intended to limit the jurisdiction of the Bill so that relevant electronic services that are not accessible to end-users in Australia would not be subject to the Bill.

Clause 14 – Designated internet service

Clause 14 inserts a definition of ***designated internet service*** which means:

- a service that allows end-users to access material using an internet carriage service; or
- a service that delivers material to persons having equipment appropriate for receiving that material, where delivery of the service is by way of an internet carriage service.

However, a designated internet service does not include:

- a social media service; or
- a relevant electronic service; or
- an on-demand program service that provides material that is identical to a program that has been or is being, transmitted on television broadcasting service. This is because it is not appropriate for the regimes established by the Bill to apply to

broadcasters who are regulated, and have to comply with licence conditions and relevant codes of practice under the BSA in relation to identical program content; or
- a service specified under subclause (2), which would allow the Minister to specify a particular internet service in the future which would not be a designated internet service; or
- an exempt service specified under subclause (3).

Subclause 14(2) allows the Minister to specify one or more services which are not a designated internet service. This allows the Minister to carve out from the definition internet services which are not appropriate to be subject to the regimes in the Bill. The Minister would do this by legislative instrument. This would be a legislative instrument for the purposes of the *Legislation Act 2003,* which accordingly must be registered in the Federal Register of Legislation, tabled in the Parliament and will be subject to Parliamentary disallowance.

Subclause 14(3) inserts a definition of an ***exempt service*** which mean services where none of the material on the service is accessible to, or delivered to, one or more end-users in Australia. This is intended to limit the jurisdiction of the Bill so that relevant electronic services that are not accessible to end-users in Australia would not be subject to the Bill.

Clause 15 – Intimate image

Clause 15 sets out the circumstances in which material would be considered ***an intimate image*** of a person for the purposes of the Act. There are three types of intimate images: depictions of a person's private parts; depictions of private activity; and depictions of a person without attire of religious or cultural significance.

Depiction of private parts

Subclause 15(2) provides that material is an intimate image of a person if the material consists of a still or moving visual image and depicts, or appears to depict, a person's genital area or anal area (whether bare or covered by underwear) or, either or both of a person's breasts if the person is a female person, or a transgender or intersex person, in circumstances in which an ordinary reasonable person would reasonably expect to be afforded privacy. This is an objective test. In most circumstances, an ordinary reasonable person would reasonably expect to be afforded privacy in relation to these types of images.

A reasonable expectation of privacy includes a reasonable expectation of control over who is permitted to observe the person in the depicted state and in what circumstances. For example, a sext (containing an image or video) sent in the context of an intimate relationship would be an intimate image. An image created for a limited audience or to be used in a limited way, such as an image of a model made available to a limited subscriber base, could also be deemed an intimate image.

The intention is for a broad interpretation of privacy so as to limit the circumstances where an image that otherwise meets the definition of 'intimate image' would be denied action by the Commissioner. However, if the image is in circumstances where an ordinary reasonable person would not reasonably expect to be afforded privacy, the image will not be deemed an intimate image. For example, an image of an underwear model taken in the course of that person's professional work where the image was created and used for a public advertising

campaign or public art display would not be an intimate image, nor would, for example, an image of a topless bather at a public beach (as opposed to a private beach).

The intention is not to capture commercial images where there has simply been a breach of copyright.

Depiction of private activity

Subclause 15(3) provides that material is an intimate image of a person if it depicts, or appears to depict, the person: in a state of undress, using the toilet, showering, having a bath, engaged in a sexual act of a kind not ordinarily done in public, or engaged in other like activity, in circumstances in which an ordinary reasonable person would reasonably expect to be afforded privacy.

The private activities listed under subparagraphs 15(3)(b)(i) to (vi) are those where an ordinary reasonable person would reasonably expect to be afforded privacy. However, if the image is in circumstances where an ordinary reasonable person would not reasonably expect to be afforded privacy, the image will not be an intimate image. For example, if an image is of a person showering using an outdoor shower facility at a public beach, the image would not be an intimate image. Where a person posts an image of themselves to a public forum and that image depicts either their private parts or themselves engaged in a private activity, that person cannot reasonably expect to be afforded privacy and, therefore, the image would not be considered an intimate image.

Depiction of person without attire of religious or cultural significance

Subclause 15(4) provides that material is an intimate image of a person if it depicts, or appears to depict, the person without religious or cultural attire that the person consistently wears in public, in circumstances in which an ordinary reasonable person would reasonably expect to be afforded privacy.

This definition recognises that an image of a person without particular religious or cultural attire that they consistently wear, can cause significant harm to the person. For example, a Muslim woman who consistently wears a niqab while in public could become significantly distressed if a picture of her without her niqab was shared. Similarly, a Sikh man who consistently wears a turban while in public, could suffer harm and distress if an image of him without his turban was shared.

Each of the above three definitions make it clear that an intimate image can be a still visual image such as a photograph, or moving visual images such as video recordings. Images could be photographs, modified photographs, animations, drawings or other depictions of the person.

Meaning of 'appear to depict'

Under each of the three definitions, an image that "appears to depict" a person would include, for example, an intimate image tagged with a person's name, implying that it is an image of that person even if it is not of them; or a highly realistic animation or digitally generated synthetic image, produced by technologies such as Generative Adversarial Networks (GANs), that purports to show a person in an intimate manner.

Paragraphs 15(2)(b) and (3)(b) and subparagraph (c)(ii) provide that to be an intimate image under any of the three definitions, the image taken must be in circumstances in which an ordinary reasonable person would reasonably expect to be afforded privacy. The listed circumstances are generally those in which an ordinary reasonable person would reasonably expect to be afforded privacy.

However, whether a circumstance is one in which an ordinary reasonable person would reasonably expect to be afforded privacy will turn on the facts and circumstances of each image. It is intended that consideration would be given to the contents of the image itself as well as the circumstances of its creation and use.

Interpretative provisions

Subclause 15(5) provides that for the purposes of this clause, it is immaterial whether material has been altered. The effect of this provision is to put it beyond doubt that an image could still be an intimate image even if it has been altered or modified. This is to cover circumstances where an image may be altered or modified to transpose one person's head on another person's body, for example, or the use of artificial technology to create highly realistic fake images, videos or audio recordings of a person, known as 'deepfakes' to create what is known as 'morph porn' or 'parasite porn'.

Subclause 15(6) makes it clear that if material depicts, or appears to depict, a part of the body of a person, the material is taken to depict the person, or appear to depict the person, as the case requires. The effect of this provision is to make it clear that the person does not need to be identifiable from the image, or for the image to include the person's face, in order to be an intimate image. For example, a depiction of a female's bare breasts and chest only, would be taken to be a depiction of the person notwithstanding that the person's face was not included in the image.

Clause 16 – Non-consensual intimate image of a person

Clause 16 provides the conditions that must be met in order for material to be considered a ***non-consensual intimate image of a person***.

This clause sets out the criteria for determining whether material submitted as part of a complaint to the Commissioner under clause 32 is a 'non-consensual intimate image of a person'.

It is intended that, in order for this test to be enlivened, the material in question must first meet the definition of 'intimate image', which is a defined term for the purposes of the Bill (see clause 15).

If the material is an intimate image as defined by clause 15, clause 16 provides 3 limbs that must be satisfied before the material meets the test for 'non-consensual intimate image of a person'. These are set out in paragraphs 16(a) to 16(c):

- the material is provided on a social media service, relevant electronic service or a designated internet service (paragraph (a));

- the person depicted did not consent to the provision of the intimate image on the service (paragraph (b)) ('consent' is a defined term for the purposes of the Bill (see clause 21)); and
- the posting of the intimate image on the service did not constitute an exempt post (paragraph (c)).

If clause 15 and all the conditions in paragraphs (a) to (c) are satisfied, clause 16 provides that the material in question is a 'non-consensual intimate image of a person'.

Clause 17 – Hosting Service

Clause 17 defines ***hosting service*** for the purposes of the Bill.

If a person (the ***first person***) hosts stored material that has been provided on a social media service, a relevant electronic service, or a designated internet service, and the first person or another person, provides one of those services on which the hosted material is provided, the hosting of the stored material by the first person is taken to be the provision of a ***hosting service*** by the first person.

The definition of hosting service covers the hosting and storage of content and data by a person in relation to those listed services. The definition of hosting service does not require the hosting service provider to be providing one of those listed services (although, often they may also provide one of the services). An example of a provision of a hosting service is where a person hosts stored material or content for a website, or for an email service.

It is noted that a search engine which merely indexes content and makes it searchable would not meet this definition of hosting service.

Clause 18 – On-demand program service

Clause 18 defines the phrase ***on-demand program service*** for the purposes of the Bill.

An on-demand program service is a service that is provided to end-users using an internet carriage service, which does no more than provide material that is identical to a program that has been, or is being, transmitted by broadcasters. Examples of on-demand program services include SBS On Demand, ABC iView and other similar applications.

When determining whether material is identical to a program, differences that are attributable to the technical characteristics of the provision or transmission are to be disregarded, as is the presence or absence of a watermark-type logo or insignia.

Subclause 18(4) is a definitional provision and provides that an expression used in paragraph 18(1)(a) will have the same meaning as it has in the BSA.

A definition of on-demand program services is required in order to exclude this type of service from the definition of designated internet service. On-demand program service material, to the extent it is identical to and also transmitted on the broadcaster's service, will be regulated under the BSA and the broadcasters would be subject to licence conditions under that Act. Accordingly, it is not appropriate for the regimes under the Bill to apply to programs

that are shown on an on-demand program service simply because they are transmitted over the internet, if those programs have, or are being, broadcast on television.

Clause 19 – Internet service providers

Clause 19 defines the phrase ***internet service providers*** for the purposes of the Bill.

An internet service provider (ISP) is a person supplying, or proposing to supply, an internet carriage service to the public. Corporate Intranets, for example, will not generally be regarded as ISPs. The concept of supply of internet carriage service to the public is dealt with in clause 20.

Subclause 19(2) provides that the Minister will, however, also have the ability to declare that a specified person who supplies, or proposes to supply, a specified internet carriage service is an ISP. This is intended primarily as an anti-avoidance mechanism, but also provides flexibility for the regime to deal with unforeseen consequences.

This declaration is a legislative instrument for the purposes of the *Legislation Act 2003,* which accordingly must be registered in the Federal Register of Legislation, tabled in the Parliament and will be subject to Parliamentary disallowance.

Clause 20 – Supply of internet carriage service to the public

Clause 20 sets out the circumstances in which an internet carriage service is deemed to be supplied to the public for the purposes of clause 19.

An internet carriage service is supplied to the public if:

- the service is used for the carriage of material between 2 end-users, both of whom are outside the immediate circle of the supplier of the service; or
- the service is used to supply point-to-multipoint services to end-users, and at least one end-user is outside the immediate circle of the supplier of the service.

Immediate circle

The concept of 'immediate circle' is defined in clause 5 to have the same meaning as in the *Telecommunications Act 1997*. Section 23 of that Act provides the principles by which a person's immediate circle may be determined.

Clause 21 – Consent

Clause 21 defines ***consent*** for the purposes of the application of this Act to an intimate image or private sexual material.

Paragraphs 21(a), 21(b) and 21(c) provide that in relation to an intimate image or private sexual material, consent must be express, voluntary, and informed. This requires consent to be clearly given for the particular instance of the provision or posting of the material, which could be verbal or in writing. This requires consent to be freely given, and not given under some kind of threat, warning, condition or consequence. It requires consent to be informed; it is expected that informed consent would include information about whom the image will be shared with, where it would be provided, and the purpose of the provision or posting.

Under the regime established by this Bill, consent will need to be in relation to the particular instance of provision or posting of the image. For example, consent to share an image with one individual would not cover the sharing of an image with a different individual. In this situation, if the person wanted to share the image with another person, further consent would be required to share the image with that other person, and that consent must be express, voluntary and informed.

Consent for the further distribution of an intimate image or private sexual material once received would also be required. That is, in circumstances where a person had received consent to share an intimate image or private sexual material with a person, if the person who received the image wanted to share that image, consent of the person depicted in the image would be required.

Paragraphs 21(d) and 21(e) set out situations when consent cannot be provided in relation to an intimate image or private sexual matter:

- Paragraph 21(d) provides that consent cannot be given by a child, who is a person under the age of 18. This is because, to the extent that the definition of intimate image overlaps with the definition of child pornography material in the Commonwealth *Criminal Code Act 1995*, a lower age of consent for the distribution of intimate images or private sexual material would create an inappropriate inconsistency between the criminal and civil frameworks. The effect of this item is that a person under the age of 18 cannot provide consent to the sharing by another person of an intimate image or private sexual image of themselves.
- Paragraph 21(e) provides that consent cannot be given by an adult who is in a mental or physical condition, whether temporary or permanent, that makes the person incapable of giving consent, or substantially impairs that person's capacity to give consent. This is to make it clear that an adult who may be unable to comprehend the concept of consent, and the consequences of sharing of the image or private sexual material, for example because they are suffering from a mental disability, cannot provide express, voluntary and informed consent.

Clause 22 – Crown to be bound

Declares that the Act binds the Crown in each of its capacities.

Clause 23 – Application of this Act

Clause 23 defines the application of the Act. Clause 23(1) extends the Bill to all of Australia's external Territories, and Clause 23(2) extends the Act to acts, omissions, matters and things outside Australia. The term 'Australia' is defined in clause 5. This provision displaces the common law presumption that statutes do not apply extraterritorially.

Clause 24 – Convention on the Rights of the Child

Clause 24 provides that the Commissioner must, as appropriate, have regard to the Convention on the Rights of the Child in the performance of functions (see clause 27) conferred by or under the Act. Subclause 24(2) confirms that subclause 24(1) does not limit the matters to which the Commissioner may have regard.

PART 2 – eSAFETY COMMISSIONER

Part 2 of the Online Safety Bill (the Bill) deals with the establishment of the eSafety Commissioner (the Commissioner) and sets out the Commissioner's powers and functions.

Clause 25 – Simplified outline of this Part

Clause 25 is a simplified outline of Part 2 of the Bill. This simplified outline is included to assist readers to understand the substantive provisions of Part 2. However, the outline is not intended to be comprehensive. It is intended that readers should rely on the substantive provisions of Part 2.

Clause 26 – eSafety Commissioner

Clause 26 establishes the statutory office of the eSafety Commissioner. The note to clause 26 indicates that, in the Bill, 'Commissioner' refers to the eSafety Commissioner, which is a term defined in clause 5 of the Bill. The same abbreviation is used in this explanatory memorandum.

Clause 27 – Functions of the Commissioner

Subclause 27(1) sets out the functions of the Commissioner.

Key functions include:

- the functions conferred by the Bill, or any other Commonwealth law or specified in the legislative rules (paragraphs (a) and (r));
- to promote online safety for Australians (paragraph (b));
- to support and encourage the implementation of measures to improve online safety for Australians (paragraph (c));
- to coordinate activities of Commonwealth Departments, authorities and agencies relating to online safety for Australians (paragraph (d));
- to collect, analyse, interpret and disseminate information relating to online safety for Australians (paragraph (e));
- to support, conduct and evaluate educational and community awareness programs relevant to online safety for Australians (paragraph (f));
- to make grants of financial assistance relating to online safety for Australians (paragraph (g));
- to conduct research about online safety for Australians (paragraph (h));
- to publish reports and papers relating to online safety for Australians (paragraph (i));
- to give the Minister reports and advice about online safety for Australians (paragraphs (j) and (k));
- to consult and cooperate with other organisations and governments about online safety for Australians (paragraph (l));
- to advise persons in relation to their obligations under the Bill (paragraph (m));
- to monitor and promote compliance with the Bill (paragraphs (n) and (o));

- to formulate and promote best practice guidelines and statements for persons and bodies involved in online safety for Australians (paragraphs (p) and (q)).

Another general function for the Commissioner is to do anything incidental or conducive to the performance of other functions (paragraph (s)). This is to clarify that the Commissioner would not be prevented from appropriate actions which would not otherwise be captured by the key functions.

Subclauses 27(2) to (4) relate to grants of financial assistance in relation to online safety for Australians that the Commissioner may make on behalf of the Commonwealth under paragraph (1)(g). The terms and conditions on which financial assistance is granted under paragraph (1)(g) are to be set out in a written agreement between the Commonwealth and the grant recipient.

Subclause 27(5) clarifies that guidelines and statements formulated under paragraph (1)(p) are not legislative instruments. Subclause 27(5) is declaratory of the law and is included to assist readers rather than create an exception to the *Legislation Act 2003*.

In performing the Commissioner's functions under clause 27, the Commissioner is expected to balance the rights and responsibilities of all stakeholders with the need to take proportionate and appropriate action in the best interests of Australians.

Clause 28 – Powers of the Commissioner

Clause 28 provides that the Commissioner has the power to do all things necessary or convenient to be done for, or in connection with, the performance of the Commissioner's functions. There is a note under clause 28 that refers to supplementary powers of the Commissioner with respect to entering into contracts, holding property and receiving money, set out at clause 178.

PART 3 - COMPLAINTS, OBJECTIONS AND INVESTIGATIONS

Part 3 of the Online Safety Bill (the Bill) provides for a complaints system for cyber-bullying material targeted at an Australian child, a complaints and objections system for non-consensual sharing of intimate images, a complaints system for cyber-abuse material targeted at Australian adult, and a complaints system relating to the online content scheme.

DIVISION 1 – Introduction

Clause 29 – Simplified outline of the Part

Clause 29 is a simplified outline of Part 3 of the Bill. This simplified outline is included to assist readers to understand the substantive provisions of Part 3. However, the outline is not intended to be comprehensive. It is intended that readers should rely on the substantive provisions of Part 3.

DIVISION 2 – Complaints about cyber-bullying material targeted at an Australian child

Clause 30 – Complaints about cyber-bullying material

Clause 30 sets out who can make a complaint about cyber-bullying material and the grounds on which a complaint may be made. 'Cyber-bullying material targeted at an Australian child', 'provided', 'parent', 'child', 'social media service', 'relevant electronic service' and 'designated internet service' are defined terms for the purposes of the Bill (see clauses 5, 6, 13, 13A and 14).

Subclause 30(1) provides that an Australian child may make a complaint to the Commissioner if the child has reason to believe that the child was or is the target of cyber-bullying material that has been, or is being, provided on a particular social media service, relevant electronic service or designated internet service.

Subclause 30(2) enables a 'responsible person' to make a complaint to the Commissioner on behalf of an Australian child if the person has reason to believe that cyber-bullying material targeted at an Australian child has been, or is being, provided on a particular social media service, relevant electronic service or designated internet service. For the purposes of subclause 30(2), a 'responsible person' is a parent or guardian of the child, or a person who the child has authorised to make a complaint on the child's behalf.

There may be circumstances under subclause 30(2) where a parent or guardian makes a complaint to the Commissioner against the wishes of the child. In such cases, it would be expected that the Commissioner would consider the child's views, consistent with the child's age and maturity, in deciding whether or not to exercise the Commissioner's discretion to investigate the complaint under clause 31.

Subclause 30(3) provides an extension of time for an adult who was an Australian child to make a complaint to the Commissioner, provided that the complaint is made within a reasonable time after the person became aware of the matter and the complaint is made within 6 months after the person reached 18 years. Such a person may make a complaint to the Commissioner if the person has reason to believe that, when the person was an Australian

child, the person was the target of cyber-bullying material that was provided on a particular social media service, relevant electronic service or designated internet service.

Evidence requirements – complaints about material provided on the service

Subclause 30(4) provides that, if a complaint made under clause 30 concerns material that has been, or is being, provided on a particular social media service, relevant electronic service or designated internet service, and the person wants the Commissioner to issue the provider of the service a removal notice (clause 65) requiring the provider to remove the material from the service; the complaint made under clause 30 must be accompanied by evidence that the material was the subject of a complaint that was previously made to the provider of the service. Where a service does not have a formal complaints-handling mechanism, evidence that an attempt has been made to report the material is acceptable (for example an email to a service provider).

Subclause 30(5) provides that, for the purposes of subclause 30(4), evidence must be in a form required by the Commissioner.

Subclauses 30(6) and 30(7) provide that the Commissioner may require evidence to be in the form of a receipt, complaint number, screen shot, statutory declaration, or another specified form in certain circumstances. However, subclauses 30(6) and 30(7) do not limit subclause 30(5) (subclause 30(8) refers).

Subclause 30(9) provides that a requirement under subclauses 30(5), 30(6) or 30(7) is not a legislative instrument. Subclause 30(9) is declaratory of the law and is included to assist readers rather than create an exception to the *Legislation Act 2003*.

Clause 31 – Investigation of complaints

Subclause 31(1) provides that the Commissioner may investigate a complaint made under clause 30. The Commissioner is not required to investigate all complaints made under clause 30 and may use discretion in deciding whether or not to investigate any particular complaint.

In some cases, the Commissioner might decline to investigate a complaint under clause 30, and instead refer the matter to a law enforcement agency in accordance with clause 224, if the Commissioner is satisfied that the material is of a sufficiently serious nature to warrant referral to a law enforcement agency in accordance with that clause.

A decision not to investigate a complaint is not reviewable under the Bill (clause 220 deals with review of decisions under the Bill). Instead, review of such a decision would be governed by the *Administrative Decisions (Judicial Review) Act 1977* and section 39B of the *Judiciary Act 1903*.

The Commissioner may choose not to investigate certain other types of complaints. For example, frivolous or vexatious or complaints which may be best resolved by the relevant school.

Subclauses 31(2) and (3) provide that an investigation under this clause is to be conducted as the Commissioner sees fit and that the Commissioner may, for the purposes of an investigation, obtain information from such persons, and make such inquiries, as the

Commissioner sees fit. It is expected that the Commissioner will develop appropriate procedures for the acceptance, investigation and closing of complaints.

Subclause 31(4) provides that subclauses 31(1) to 31(3) have effect subject to Part 14 of the Bill which confers certain investigative powers on the Commissioner.

Subclause 31(5) provides that the Commissioner may terminate an investigation made under clause 31. This could occur, for example, in circumstances where the Commissioner commenced an investigation and, based on initial inquiries, determined that the complaint did not have any merit. The Commissioner might also decide to terminate an investigation where the matter is of a criminal nature and would be better dealt with by police. Under clause 224, the Commissioner must refer material to a law enforcement agency if the Commissioner is satisfied that the material is of a sufficiently serious nature.

DIVISION 3 – Complaints about, and objections to, intimate images

Clause 32 – Complaints

Clause 32 allows a person who is the subject of an intimate image (the 'depicted person') to make a complaint to the Commissioner if they believe the image has been shared without their consent on a social media service, relevant electronic service or designated internet service. 'Intimate image' is a defined term for the purpose of the Bill (see clause 15).

The provision makes it clear that the person can make a complaint even if they are not able to identify the person who allegedly shared the image without consent, however they must include a statement to this effect when making a complaint to the Commissioner (subclause 32(2)). This reflects that subjects of non-consensual sharing of intimate images may not always know the perpetrator, for example because the image may have been shared by several people. This provision is intended to also assist the Commissioner in deciding which type of removal notice to issue, should the Commissioner decide to exercise these powers, as removal notices can be issued to end-users (clause 78); providers of social media services, relevant electronic services, or designated internet services (clause 77); or to hosting service providers (clause 79).

Subclause 32(3) provides for an authorised person to make a complaint to the Commissioner on behalf of a person who is the subject of an intimate image, in limited circumstances (clause 32(3)). Those circumstances are:

- The person depicted in the image has authorised, verbally or in writing, the person to make a complaint about the matter (paragraph 32(3)(a)). An example of a situation where a complaint may be made by an authorised person is where the depicted person wishes to remain anonymous to minimise further distress when going through the process, and they authorise someone they trust to make the complaint on their behalf. Another example where a person may be authorised to make a complaint is where a child authorises an older sibling to make a complaint on their behalf.
- The person depicted in the image is a child under the age of 16 years, and the authorised person is a parent or guardian of the depicted person (paragraph 32(3)(b)). In these circumstances, the child is not required to authorise the parent or guardian to make a complaint and the parent or guardian can make a complaint (noting under the

definition of consent in proposed clause 21, a child under the age of 18 cannot provide consent to share an intimate image).

- The person depicted in the image is in a mental or physical condition, whether temporary or permanent, that makes the person incapable of managing their affairs, and the authorised person is a parent or guardian of the depicted person (paragraph 32(3)(c)). In these circumstances, the person is not required to authorise the parent or guardian to make a complaint. The parent or guardian can make a complaint if the person is incapable of managing their own affairs and there has been a contravention of the prohibition on the non-consensual sharing of an intimate image.

If an authorised person is making a complaint, the authorised person must make a declaration to the Commissioner indicating that the person is entitled to make the complaint on behalf of the person depicted in the image (subclause 32(4)).

Similar to subclause 32(2), the authorised person can make a complaint even if they are not able to identify the person who allegedly shared the image without consent, however they must include a statement to this effect when making a complaint to the Commissioner (subclause 32(5)).

Clause 33 – Objection Notice

Clause 33 allows a person who is the subject of an intimate image to give an objection notice to the Commissioner in relation to that image. An 'objection notice' is a defined term for the purpose of the Bill (see clause 5).

The criteria for the giving of an objection notice by a person to the Commissioner are:

- The intimate image is, or has been, provided on a social media service, a relevant electronic service, or a designated internet service (paragraph 33(1)(a)) ; and
- The provision of the intimate image on the service did not constitute an exempt provision, as defined in clause 86 (paragraph 33(1)(b)); and
- There was one of three possible links to Australia, which would be satisfied: the depicted person is ordinarily resident in Australia, the end-user who posted the image on the service (if there is one) is ordinarily resident in Australia, or the intimate image is hosted in Australia by a hosting service (paragraph 33(1)(c)).

An objection notice made under clause 33 differs to a complaint made under clause 32 in that the person may give an objection notice to the Commissioner even if the depicted person previously consented to the provision of the intimate image on the service (subclause 33(2)). That is, an objection notice can be given to the Commissioner even if there was no breach of the prohibition contained in proposed clause 75 of the Bill. One of the purposes of the objection notice is to provide an avenue to seek removal of intimate images that a person may subsequently regret having provided consent to share the image, or the person is suffering distress or harm that was not foreseen at the time they provided consent.

If the criteria for the giving of an objection notice in relation to another person have been met, clause 33 would also provide for an authorised person to make a complaint to the Commissioner on behalf of a person who is depicted in the intimate image that has allegedly been shared, in limited circumstances (paragraph 33(3)(e)). Those circumstances are:

- The person depicted in the image has authorised, verbally or in writing, the person to give an objection notice to the Commissioner (paragraph 33(3)(d)). An example of a situation where an objection notice may be given by an authorised person is where the depicted person wishes to remain anonymous to minimise further distress, and they authorise someone they trust to give the objection notice on their behalf.
- The person depicted in the image is a child under the age of 16 years, and the authorised person is a parent or guardian of the depicted person (paragraph 33(3)(e)). In these circumstances, the child is not required to authorise the parent or guardian to give the objection notice, the parent or guardian can give the notice if a child is under the age of 16 and a person has shared an intimate image of the child.
- The person depicted in the image is in a mental or physical condition, whether temporary or permanent, that makes the person incapable of managing their affairs, and the authorised person is a parent or guardian of the depicted person (paragraph 33(3)(f)). In these circumstances, the person is not required to authorise the parent or guardian to give the objection notice. The parent or guardian can give the notice if the person is incapable of managing their own affairs and an intimate image has been shared.

Subclause 33(4) provides that, if an authorised person is giving an objection notice to the Commissioner, the authorised person must make a declaration to the Commissioner indicating that the person is entitled to give the notice on behalf of the person depicted in the image.

Subclause 33(5) provides that an authorised person may give an objection notice to the Commissioner even if the depicted person previously consented to the provision of the intimate image on the service. This reflects that the intention of the objection notices is to provide an avenue for people to seek removal of intimate images, even if they consented to the sharing of the image in the past.

Clause 34 – Investigation of complaints

Clause 34 provides the Commissioner with the discretion to investigate a complaint made under clause 32. The discretionary nature of this power provides flexibility to the Commissioner to decide which complaints can be investigated, and will allow the Commissioner to appropriately direct resources to where they are needed most.

The proposed provision makes it clear that the Commissioner may conduct an investigation, obtain information, and make such inquiries as the Commissioner sees fit (subclause 34(2)). This reflects the intention that the Commissioner should be able to conduct any investigation in a manner the Commissioner considers appropriate. It is expected that the Commissioner will develop appropriate procedures for the acceptance, investigation and closing of complaints.

These powers of the Commissioner have effect subject to Part 14 which provides the Commissioner with certain investigative powers (subclause 34(4)). Those powers include the power to summon persons to attend before the Commissioner, or a delegate, to provide a document or answer questions, examine a person under oath or affirmation, or require the production of documents for inspection. These powers provide appropriate information

gathering powers for the Commissioner to utilise in any investigation undertaken under clause 34.

The proposed provision also makes it clear that the Commissioner may terminate an investigation under this clause (subclause 34(5)). The effect of this provision is that after the Commissioner commences an investigation, that investigation may later be terminated at the Commissioner's discretion. This could occur, for example, in circumstances where the Commissioner commenced an investigation and, based on initial inquiries, determined that the complaint did not have any merit. The Commissioner might also decide to terminate an investigation where the matter is of a criminal nature and would be better dealt with by police. Under clause 224, the Commissioner must refer material to a law enforcement agency if the Commissioner is satisfied that the material is of a sufficiently serious nature.

Clause 35 – Commissioner's response to objection notices

Clause 35 provides that if an objection notice is given to the Commissioner under clause 33 in relation to an intimate image, the Commissioner may consider whether to give a removal notice in relation to the image.

The effect of this provision is to make it clear that if the Commissioner has received an objection notice under clause 33, the Commissioner has the discretion to decide whether to give a removal notice under clauses 77, 78 or 79 in relation to the intimate image. The discretionary nature of this power provides flexibility to the Commissioner to decide when objection notices will be considered, allowing resources to be directed to where they are needed most.

DIVISION 4 – Complaints about cyber-abuse material targeted at an Australian adult

Clause 36 – Complaints about cyber-abuse material

Clause 36 of the Bill sets out who can make a complaint about cyber-abuse material and the grounds on which a complaint may be made. 'Cyber-abuse material targeted at an Australian adult' and 'target' are defined terms for the purposes of the Bill (see clause 5 and clause 6).

Subclause 36(1) provides that an Australian adult may make a complaint to the Commissioner if the adult has reason to believe that they were, or are, the target of cyber-abuse material that has been, or is being, provided on a particular social media service, relevant electronic service or designated internet service.

Subclause 36(2) enables a responsible person to make a complaint to the Commissioner on behalf of an Australian adult if the person has reason to believe that cyber-abuse material targeted at an Australian adult has been, or is being, provided on a particular social media service, relevant electronic service or designated internet service. For the purposes of subclause 36(2), a 'responsible person' is a person whom the adult has authorised to make a complaint on their behalf.

An example of a situation where a responsible person may make the complaint on behalf of an adult is where the target wishes to remain anonymous to minimise further distress, and they authorise someone they trust to give the complaint on their behalf.

Evidence requirements – complaints about material provided on a service

Subclause 36(3) provides that, if a complaint made under clause 36 concerns material that has been, or is being, provided on a particular social media service, relevant electronic service or designated internet service, and the person wants the Commissioner to issue the provider of the service a removal notice (clause 90) requiring the provider to remove the material from the service; the complaint made under clause 36 must be accompanied by evidence that the material was the subject of a complaint that was previously made to the provider of the service. Where a service does not have a formal complaints-handling mechanism, evidence that an attempt has been made to report the material is acceptable (for example an email to a service provider).

Subclause 36(4) provides that, for the purposes of subclause 36(3), evidence must be in a form required by the Commissioner.

Subclauses 36(5) and 36(6) provide that the Commissioner may require evidence to be in the form of a receipt, complaint number, screen shot, statutory declaration, or another specified form in certain circumstances. However, subclauses 36(5) and 36(6) do not limit subclause 36(4) (subclause 36(7) refers).

Subclause 36(8) provides that a requirement under subclauses 36(4), 36(5) or 36(6) is not a legislative instrument. Subclause 36(8) is declaratory of the law and is included to assist readers rather than create an exception to the *Legislation Act 2003*.

Clause 37 – Investigation of complaints

Subclause 37(1) provides that the Commissioner may investigate a complaint made under clause 36. The Commissioner is not required to investigate all complaints made under clause 36 and may use discretion in deciding whether or not to investigate any particular complaint.

In some cases, the Commissioner might decline to investigate a complaint under clause 36, and instead refer the matter to a law enforcement agency if the Commissioner is satisfied that the material is of a sufficiently serious nature to warrant referral to a law enforcement agency in accordance with clause 224.

A decision not to investigate a complaint is not reviewable under the Bill (clause 220 deals with review of decisions under the Bill). Instead, review of such a decision would be governed by the *Administrative Decisions (Judicial Review) Act 1977* and section 39B of the *Judiciary Act 1903*.

The Commissioner may choose not to investigate certain other types of complaints, for example, complaints which are frivolous or vexatious or complaints where it is clear that the material in question does not meet the threshold of cyber-abuse material.

Subclauses 37(2) and (3) provide that an investigation under this clause is to be conducted as the Commissioner sees fit, and that the Commissioner may, for the purposes of an investigation, obtain information from such persons, and make such inquiries, as the Commissioner sees fit. It is expected that the Commissioner will develop appropriate procedures for the acceptance, investigation and closing of complaints.

Subclause 37(4) provides that subclauses 37(1) to 37(3) have effect subject to Part 14 of the Bill, which confers certain investigative powers on the Commissioner.

Subclause 37(5) provides that the Commissioner may terminate an investigation made under clause 37. This could occur, for example, in circumstances where the Commissioner commenced an investigation and, based on initial inquiries, determined that the complaint did not have any merit. The Commissioner might also decide to terminate an investigation where the matter is of a criminal nature and would be better dealt with by police. Under clause 224, the Commissioner must refer material to a law enforcement agency if the Commissioner is satisfied that the material is of a sufficiently serious nature.

DIVISION 5 – Complaints relating to the online content scheme

Clause 38 – Complaints about class 1 material or class 2 material

Clause 38 sets out who can make a complaint about class 1 material or class 2 material, and the grounds on which a complaint may be made. 'Class 1 material' and 'class 2 material' are defined terms for the purposes of the Bill (see clause 106 and clause 107).

Subclause 38(1) provides that a person may make a complaint to the Commissioner if they have reason to believe that end-users in Australia can access class 1 material or class 2 material covered by paragraph 107(1)(a), (b), (c), (d) or (e) on a social media service, relevant electronic service or designated internet service.

Subclause 38(2) provides that a person may make a complaint to the Commissioner if they have reason to believe that end-users in Australia can access class 2 material covered by 107(1)(f), (g), (h), (i), (j), (k) or (l) on a social media service, relevant electronic service or designated internet service, and access to the material is not subject to a restricted access system.

Clause 39 – Complaints relating to breach of a service provider rule etc.

Clause 39 provides that a person may make a complaint to the Commissioner about another person if they have reason to believe that that person has breached a service provider rule that applies to that person, or a civil penalty provision of Part 9 of the Bill. Under clause 151, the Minister may establish service provider rules by legislative instruments to apply to particular service providers. For example, a person may make a complaint to the Commissioner if they have reason to believe that a service provider has breached a service provider rule that applies to that provider.

Clause 40 – Complaints relating to breach of an industry code etc.

Clause 40 provides that a person may make a complaint to the Commissioner about a participant of the online industry (within the meaning of Division 7 of Part 9), if they have reason to believe that that participant has breached a code or an industry standard registered under that Division that is applicable to the participant. For example, a person may make a complaint that a particular service provider within the online industry has not addressed the presence of harmful content on its service in a manner that is appropriate for fulfilling its obligations under a code or industry standard that applies to it.

Clause 41 – Residency etc. of complainant

Clause 41 provides that the complainant must be resident in Australia, or a body corporate that carries on activities in Australia, the Commonwealth, a State or a Territory. This is so that there is an appropriate connection to Australia for the purposes of the Commissioner exercising their powers.

Clause 42 – Commissioner may investigate matters

Subclause 42(1) provides that the Commissioner may investigate matters.

The Commissioner may commence an investigation either on the Commissioner's own initiative or in response to a complaint made under clauses 38, 39, or 40. The Commissioner is not required to investigate all complaints made under clauses 38, 39 and 40 and may use discretion in deciding whether or not to investigate any particular complaint.

Subclauses 42(2) and (3) provide that an investigation under this clause is to be conducted as the Commissioner sees fit, and that the Commissioner may, for the purposes of an investigation, obtain information from such persons, and make such inquiries, as the Commissioner sees fit. It is expected that the Commissioner will develop appropriate procedures for the acceptance, investigation and closing of complaints.

Subclause 42(4) provides that subclauses 42(1) to 42(3) have effect subject to Part 14, which confers certain investigative powers on the Commissioner.

Clause 43 – Commissioner may refuse to investigate certain matters

Clause 43 provides that, in some cases, the Commissioner might decline to investigate a complaint under clause 38, 39 or 40. Subclause 43(1) provides that, ordinarily, the Commissioner may decline to investigate a matter if the complainant could have made a complaint under a registered industry code or standard determined under Division 7 of Part 9. However, subclause 43(2) provides that subclause 43(1) does not limit the circumstances in which the Commissioner may refuse to investigate a matter.

PART 4 – BASIC ONLINE SAFETY EXPECTATIONS

Part 4 of the Online Safety Bill (the Bill) provides the Minister the power to determine basic online safety expectations for social media services, relevant electronic services and designated internet services. Part 4 of the Bill also provides the Commissioner the power to require providers of a social media service, relevant electronic service or designated internet service to report about their compliance with the applicable basic online safety expectations.

DIVISION 1 – Introduction

Clause 44 – Simplified outline of this Part

Clause 44 is a simplified outline of Part 4 of the Bill. This simplified outline is included to assist readers to understand the substantive provisions of Part 4. However, the outline is not intended to be comprehensive. It is intended that readers should rely on the substantive provisions of Part 4.

DIVISION 2 – Basic online safety expectations

Clause 45 – Basic online safety expectations

Clause 45 provides the Minister with the power to determine, by legislative instrument, basic online safety expectations for a social media service, relevant electronic service, or designated internet service. 'Social media service', 'relevant electronic service', or 'designated internet service' are defined terms for the purposes of the Bill (see clauses 5, 13, 13A and 14).

The basic online safety expectations will be a set of expectations that the Australian Government expect service providers to meet in order to uphold the safety of Australian end-users on their services, but also allow them flexibility in the method of achieving these expectations. An example of how a service provider might do so is by updating the service's terms of use to include standards of end-user behaviour, or to prohibit cyber-bullying, cyber-abuse, the non-consensual sharing of intimate images, material that depicts, promotes, incites or instructs in abhorrent violent conduct, class 1 material and class 2 material, and other harmful material from the service.

'Other harmful material' is intended to capture emerging forms of harmful material and behaviours. This may include, for example, high volume, cross-platform attacks (also known as 'volumetric' or 'pile-on' attacks). This is a circumstance where a person is named in, tagged, or otherwise linked to an abusive post, which others like, share, re-post with additional commentary, and link to via other services. Individual pieces of material in an attack may not reach the threshold for cyber-bullying or cyber-abuse, however, as the volume of material can proliferate rapidly across platforms, with hundreds or thousands of related posts focused on a single individual. Other harmful material might also include an end-user posting an image or video of a second person that uses artificial intelligence technology to transpose the second person's head on a computer-generated body (known as a 'deepfake'), for the purpose of misrepresenting the second person. Such an image may invite cyber-bullying, cyber-abuse, or a volumetric attack against the second person. Service providers are best placed to identify these emerging forms of harmful end-user conduct or material, and so the flexibility of this regime means that providers can choose the best way to address them on their service in the most responsive way.

Subclause 45(4) provides that a determination made by the Minister under clause 45 does not impose a duty that is enforceable by proceedings in a court.

A determination is a legislative instrument for the purposes of the *Legislation Act 2003,* which accordingly must be registered in the Federal Register of Legislation, tabled in the Parliament and will be subject to Parliamentary disallowance.

Clause 46 – Core expectations

Subclause 46(1) provides that a determination made under clause 45 must specify certain expectations at a minimum, as listed in paragraphs 46(1)(a)-(i). The core expectations are principles-based and should be read in their broadest sense. The intention is for the core expectations to apply to all social media services and all members of the defined classes of designated internet services and relevant electronic services.

Paragraph 46(1)(a) lists as a core expectation that the provider of the service will take reasonable steps so that end-users are able to use the service in a safe manner, and paragraph 46(1)(b) lists as a core expectation that the provider of the service will consult with the Commissioner to determine what reasonable steps means for that provider. This could be by seeking the advice of the Commissioner or following guidance issued by the Commissioner on the core expectations listed in paragraphs 46(1)(a)-(i) as well in relation to a determination made under clause 45.

Paragraph 46(1)(c) lists as a core expectation that the provider of the service must take reasonable steps to minimise the extent to which the following materials are provided on their services:

- cyber-bullying material targeted at an Australian child;
- cyber-abuse material targeted at an Australian adult;
- non-consensual intimate images of a person;
- class 1 material;
- material that promotes abhorrent violent conduct;
- material that incites abhorrent violent conduct;
- material that instructs in abhorrent violent conduct; and
- material that depicts abhorrent violent conduct.

For example, setting clear minimum standards for online behaviour relating to the posting of the materials listed in paragraph 46(1)(c) and establishing clear protocols and consequences for service violations, including account suspension, access restrictions and blocking repeat offenders, would be considered a reasonable step in meeting this expectation.

Paragraph 46(1)(d) lists as a core expectation that the provider of a service will take reasonable steps to ensure that technological or other measures are in effect to prevent access by children to class 2 material provided on the service.

Paragraph 46(1)(e) lists as a core expectation that the provider of a service will ensure that the service has clear and readily identifiable mechanisms that enable end-users to report, and make reports about, material listed in paragraph 46(1)(e), as well as similar mechanisms to report breaches of the service's terms of use (paragraph 46(1)(f)). For example, complaints

and reporting systems that are accessible, fair, responsive and effective in dealing with reports of harmful content and conduct would likely meet this core expectation.

Paragraphs 46(1)(g), 46(1)(h) and 46(1)(i) provide that, as a core expectation, the provider is expected to report to the Commissioner within 30 days of receiving a request seeking the number of breaches of the service's terms of use (paragraph 46(1)(g)) within a set period; how long the provider took to respond to any removal notices issued to it by the Commissioner under the Act during a set period (paragraph 46(1)(h)); and what measures the provider is taking to provide for end-users to use their service safely (paragraph 46(1)(i)).

Subclause 46(2) provides that determinations made under clause 45 are not limited to the expectations listed in subclause 46(1). The effect of this provision is to provide the Minister with the power to include further expectations in determinations made under clause 45.

Service providers that can demonstrate they have the necessary capabilities (both technology and human), skills, processes, systems and scalable solutions to respond to online harms occurring on their service would likely meet these core expectations. For example, embedding user safety considerations, training and practices into the roles, functions and working practices of those employed by the provider and putting in place preventative measures to detect, surface, hash (where applicable), flag and remove illegal and harmful conduct and content would also be considered a reasonable step in meeting the core expectations.

Clause 47 – Consultation

Clause 47 provides that, before the Minister determines or makes a major variation to the basic online safety expectations under clause 47, the Minister must make a copy of the draft determination available on the Department's website and publish a notice seeking public comment on the draft. The effect of this clause is to allow industry and the public to comment on the determination, and to raise any issues or concerns for the Government's consideration prior to the determination being made. Subclause 47(2) provides that the consultation period must run for at least 30 days after the publication of the notice and the Minister must have due regard to any comments made (subclause 47(4)).

Clause 48 – Service provider notifications

Clause 48 provides that, if there are basic online safety expectations for a social media service, relevant electronic service, or designated internet service, and if the provider of the service either contravenes one or more of those expectations (subclause 48(2)), or complies with those expectations (subclause 48(3)), the Commissioner may prepare a statement to that effect. The Commissioner must provide a copy of that statement to the provider in question, and, if the Commissioner considers it appropriate to do so, may also publish that statement on the Commissioner's website.

The intention of this clause is to introduce a reputational risk for providers to incentivise compliance with the Australian Government's basic online safety expectations applicable to them. It also introduces the possibility of positive reinforcement, so that the Commissioner can notify the public of a provider's good standing.

DIVISION 3 – Reporting

Division 3 provides the Commissioner with powers to require providers of social media services, relevant electronic services, or designated internet services to report on their compliance with the basic online safety expectations relevant to their service.

There are four clauses that relate to these powers:

- a periodic report notice made under clause 49, which requires an individual provider to report to the Commissioner on their compliance with the basic online safety expectations relevant to their service multiple times at regular intervals;
- a periodic report determination made under clause 52, which requires each provider within a class of providers to report multiple times at regular intervals;
- a non-periodic report notice issued under clause 56, which requires an individual provider to prepare only a single report to be given to the Commissioner;
- a non-periodic report determination made under clause 59, which requires each provider within a class of providers to each prepare a report to be given to the Commissioner.

The purpose of these reporting powers is to deliver the Government's commitment to hold major social media platforms and other technology firms to account by mandating transparency reports on the number and type of response to reports and complaints about illegal abusive and predatory content by their users.

For each, the Commissioner will have the power to require the provider to report on either their compliance with all basic online safety expectations relevant to their service or on their compliance with one or more specified basic online safety expectations relevant to their service. The provider must prepare the report in the manner and form specified in the Commissioner's notice, and give the report to the Commissioner either within the time period specified in the report, or such longer period as the Commissioner allows (but not less than 28 days).

In deciding whether to issue a notice, clauses 49 and 56 also require the Commissioner to consider the number of complaints under this Bill, contraventions of this Part, the provider's practices or terms of use, and their reporting history. The effect of this is for the Commissioner to consider the value of the regulatory burden that would be imposed on the provider if the Commissioner should require them to report, especially if there is no reason for the Commissioner to suspect that the provider is acting in contravention of the Bill. This is intended to allow the Commissioner to put the resources available to the Commissioner to the best use, by providing the Commissioner with a decision framework to limit which providers the Commissioner may require to report. Clauses 52 and 59 do not include this requirement.

Subdivision A – Periodic reporting about compliance with basic online safety expectations

Clause 49 – Periodic reporting notice

Clause 49 provides that, where a social media service, relevant electronic service or designated internet service is subject to basic online safety expectations, the Commissioner may, by written notice, require the provider of the service to prepare periodic reports about the provider's compliance with those expectations.

Clause 50 – Compliance with notice

Clause 50 provides that a person must comply with a reporting notice issued under clause 49(2) to the extent that the person is capable of doing so.

This is a civil penalty provision, and 500 penalty units attach to a contravention of this provision.

Civil penalty provisions are enforceable under Part 4 of the *Regulatory Powers (Standard Provisions) Act 2014* (Regulatory Powers Act), in accordance with subclause 162(1) of the Bill. If a person refuses to comply with a reporting notice, daily penalties for contraventions of clause 50 would apply under section 93 of the Regulatory Powers Act.

In addition to the court ordered civil penalty, the Commissioner has access to other enforcement options. Clause 163 provides that this provision is subject to an infringement notice. Clause 164 provides that this provision is subject to enforceable undertakings. Clause 165 provides that this provision is subject to injunctions.

Clause 51 – Formal warning

Clause 51 enables the Commissioner to issue a formal warning if a person contravenes clause 50.

This is an alternative mechanism available to the Commissioner of taking other enforcement action. A formal warning provides a lighter touch mechanism which the Commissioner may choose to use. The Commissioner may issue a formal warning instead of pursuing a civil penalty order or issuing an infringement notice where, for example, it is the first contravention by the person. Whether a formal warning is issued instead of or in addition to taking other enforcement action is a decision for the Commissioner.

Clause 52 – Periodic reporting determination

Clause 52 provides that, if there are basic online safety expectations for a social media service, relevant electronic service, or designated internet service, the Commissioner may, by legislative instrument, determine that each provider of a service within a specified class of services must prepare periodic reports about the provider's compliance with those expectations.

A determination is an legislative instrument for the purposes of the *Legislation Act 2003,* which accordingly must be registered in the Federal Register of Legislation, tabled in the Parliament and will be subject to Parliamentary disallowance.

Clause 53 – Compliance with determination

Clause 53 provides that a person must comply with a determination made under subclause 52(2) to the extent that they are capable of doing so.

This is a civil penalty provision, and 500 penalty units attach to a contravention of this provision. Civil penalty provisions are enforceable under Part 4 of the Regulatory Powers Act, in accordance with subclause 162(1) of the Bill.

In addition to the court ordered civil penalty, the Commissioner has access to other enforcement options. Clause 163 provides that this provision is subject to an infringement notice. Clause 164 provides that this provision is subject to enforceable undertakings. Clause 165 provides that this provision is subject to injunctions.

Clause 54 – Formal warning

Clause 54 allows the Commissioner to issue a formal warning if a person contravenes clause 53.

This is an alternative mechanism available to the Commissioner instead of taking other enforcement action. A formal warning provides a lighter touch mechanism which the Commissioner may choose to use. The Commissioner may issue a formal warning instead of pursuing a civil penalty order or issuing an infringement notice where, for example, it is the first contravention by the person. Whether a formal warning is issued instead of or in addition to taking other enforcement action is a decision for the Commissioner.

Clause 55 – Service provider notifications

Clause 55 provides that, if a provider does not comply with a notice or a determination that requires them to report under clauses 49 or 52, the Commissioner may prepare a statement to that effect. The Commissioner may provide a copy of that statement to the provider in question and publish that statement on the Commissioner's website.

The intention of clause 55 is to introduce a reputational risk for providers, to provide a further incentive to comply with a determination or reporting notices issued by the Commissioner, in addition to the penalties established by clauses 50 and 53. It also introduces the possibility of positive reinforcement – if a provider is compliant, the Commissioner can notify the public of that provider's good standing.

Subdivision B – Non-periodic reporting about compliance with basic online safety expectations

Clause 56 – Non-periodic reporting notice

Clause 56 provides that, if there are basic online safety expectations for a social media service, relevant electronic service, or designated internet service, the Commissioner may, by written notice, require the provider of the service to prepare a report about the provider's compliance with those expectations.

Clause 57 – Compliance with notice

Clause 57 provides that a person must comply with a reporting notice issued under subclause 56(2) to the extent that they are capable of doing so.

This is a civil penalty provision, and 500 penalty units attach to a contravention of this provision. Civil penalty provisions are enforceable under Part 4 of the Regulatory Powers Act, in accordance with subclause 162(1) of the Bill. If a person refuses to comply with a reporting notice, daily penalties for contraventions of clause 57 would apply under section 93 of the Regulatory Powers Act.

In addition to the court ordered civil penalty, the Commissioner has access to other enforcement options. Clause 163 provides that this provision is subject to an infringement notice. Clause 164 provides that this provision is subject to enforceable undertakings. Clause 165 provides that this provision is subject to injunctions.

Clause 58 – Formal warning

Clause 58 allows the Commissioner to issue a formal warning if a person contravenes clause 57.

This is an alternative mechanism available to the Commissioner instead of taking other enforcement action. A formal warning provides a lighter touch mechanism which the Commissioner may choose to use. The Commissioner may issue a formal warning instead of pursuing a civil penalty order or issuing an infringement notice where, for example, it is the first contravention by the person. Whether a formal warning is issued instead of or in addition to taking other enforcement action is a decision for the Commissioner.

Clause 59 – Non-periodic reporting determination

Clause 59 provides that, if there are basic online safety expectations for a social media service, relevant electronic service, or designated internet service, the Commissioner may, by legislative instrument, determine that each provider of the service in the specified class of service to each prepare a report about the provider's compliance with those expectations.

A determination is a legislative instrument for the purposes of the *Legislation Act 2003,* which accordingly must be registered in the Federal Register of Legislation, tabled in the Parliament and would be subject to Parliamentary disallowance.

Clause 60 – Compliance with determination

Clause 60 provides that a person must comply with a determination made under subclause 59(2) to the extent that they are capable of doing so.

This is a civil penalty provision, and 500 penalty units attach to a contravention of this provision. Civil penalty provisions are enforceable under Part 4 of the Regulatory Powers Act, in accordance with subclause 162(1) of the Bill. If a person refuses to comply with a reporting notice, daily penalties for contraventions of clause 59(2) would apply under section 93 of the Regulatory Powers Act.

In addition to the court ordered civil penalty, the Commissioner has access to other enforcement options. Clause 163 provides that this provision is subject to an infringement notice. Clause 164 provides that this provision is subject to enforceable undertakings. Clause 165 provides that this provision is subject to injunctions.

Clause 61 – Formal warning

Clause 61 allows the Commissioner to issue a formal warning if a person contravenes clause 60.

This is an alternative mechanism available to the Commissioner instead of taking other enforcement action. A formal warning provides a lighter touch mechanism which the Commissioner may choose to use. The Commissioner may issue a formal warning instead of pursuing a civil penalty order or issuing an infringement notice where, for example, it is the first contravention by the person. Whether a formal warning is issued instead of or in addition to taking other enforcement action is a decision for the Commissioner.

Clause 62 – Service provider notifications

Clause 62 provides that, if a provider does not comply with a notice or a determination that requires them to report under clauses 56 or 59, the Commissioner may prepare a statement to that effect. The Commissioner may provide a copy of that statement to the provider in question, and publish that statement on the Commissioner's website.

The intention of clause 62 is to introduce a reputational risk for providers, to provide a further incentive to comply with a determination or reporting notice issued by the Commissioner, in addition to the penalties established by clauses 57 and 60. It also introduces the possibility of positive reinforcement – if a provider is compliant, the Commissioner can notify the public of that provider's good standing.

Subdivision C – Self-incrimination

Clause 63 – Self-incrimination

Clause 63 provides that a person will not be excused from giving any of the reports about compliance with the basic online safety expectations that might be required under Division 3 of Part 4 of the Bill by claiming that complying will either self-incriminate them, or that they will expose themselves to a penalty.

Clause 63 provides that compliance with a reporting requirement under Division 3 may not be used as evidence in a civil proceeding for the recovery of a penalty (other than proceedings for the recovery of a penalty under Division 3); or in criminal proceedings against the person (other than proceedings for an offence against section 137.1 or 137.2 of the Criminal Code that relates to this Part).

Sections 137.1 and 137.2 of the Criminal code include offences about the production of false or misleading information or documents.

The effect of this clause is to enable the person to comply with a reporting requirement under Division 3 without that compliance being used against them in another civil or criminal matter. The purpose of the clause is to facilitate the provision of identity information or contact details about an end-user where the Commissioner believes on reasonable grounds that the information is, or the contact details are, relevant to the operation of the Bill.

PART 5 – CYBER BULLYING MATERIAL TARGETED AT AN AUSTRALIAN CHILD

Part 5 of the Online Safety Bill (the Bill) deals with the treatment of cyber-bullying material targeted at an Australian child.

Clause 64 – Simplified outline of this Part

Clause 64 is a simplified outline of Part 5 of the Bill. It provides that removal notices may be given to a provider of a social media service, relevant electronic service or designated internet service or to a hosting service provider requiring them to remove or cease hosting the cyber-bullying material. It also provides that an end-user notice may be given to a person who posts cyber-bullying material, requiring them to do any or all of the following: take reasonable steps to remove the material; refrain from posting cyber-bullying material; or apologise for posting the material.

'Cyber-bullying material directed at an Australian child', 'provided', 'parent', 'child', 'social media service', 'relevant electronic service', 'designated internet service' and 'hosting service provider' are defined terms for the purposes of the Bill (see clauses 5, 6, 13, 13A, 14 and 17).

This simplified outline is included to assist readers to understand the substantive provisions of Part 5. However, the outline is not intended to be comprehensive. It is intended that readers should rely on the substantive provisions of Part 5.

Clause 65 – Removal notice given to the provider of a social media service, relevant electronic service or designated internet service

Clause 65 provides the Commissioner with the power, in certain circumstances, to give the provider of a social media service, a relevant electronic service or a designated internet service a notice requiring the provider to remove cyber-bullying material targeted at an Australian child that was provided on the service. 'Removal notice' is a defined term for the Bill (clause 5). The circumstances in which material is provided on a service are defined in clause 10.

The Bill provides for these notices to be given to service providers, as they are considered to be best placed to quickly remove the cyber-bullying material from their particular service and reduce the harm suffered by the target of the cyber-bullying material.

Before the Commissioner can give a removal notice in relation to cyber-bullying material, there must be a complaint made to the Commissioner about the material under clause 30. This is so the Commissioner's power is only enlivened if the target of the material has complained.

Paragraphs 65(b)-(c) establish a pre-condition for a removal notice that the complainant had first complained to the service provider, and that the material was not removed. Many large service providers facilitate complaints handling on their services. The intention is to provide the service provider with an opportunity to address any breach of the service's terms of use through its normal processes, prior to any intervention by the Commissioner.

Subclause 65(2) includes a requirement that the notice must so far as reasonably practicable, identify the particular material to be removed a way that enables the service provider to

comply. This is intended to include for example a URL or particular website where the material is to be found. This is so that the service provider is able to quickly locate, and remove the material in compliance with the notice.

The removal notice would require the provider to remove the cyber-bullying material from the service within 24 hours or any longer period as allowed by the Commissioner. The period of 24 hours reflects that the primary concern of the target of the cyber-bullying material is often the removal of the material as quickly as possible.

If the Commissioner decides not to issue a removal notice to the service provider, subclause 65(3) would also require the Commissioner to give written notice of the refusal to the person who made the complaint in relation to cyber-bullying material. It is expected that the Commissioner would also include reasons why the notice was not issued in the circumstances.

An application may be made to the Administrative Appeals Tribunal (AAT), by either the provider of the service concerned or the end-user who posted the material, for review of a decision of the Commissioner to give a removal notice under clause 65 (subclauses 220(2) and (3) refer). The AAT can also, on application, review a decision of the Commissioner to refuse to give a removal notice (subclauses 220(4) and (5) refer).

Clause 66 – Removal notice given to a hosting service provider

Clause 66 provides the Commissioner with the power, in certain circumstances, to give a hosting service provider a notice requiring the provider to remove cyber-bullying material targeted at an Australian child from the service.

Clause 66 reflects the same principles and processes as clause 65, however is directed at a hosting service provider rather than at a provider of a social media service, relevant electronic service or designated internet service. This is to allow for circumstances where the hosting service provider is best placed to remove the material, or circumstances where the Commissioner may require material to be removed from more than one location. For instance, if an end-user has posted cyber-bullying material onto a service, and a hosting service has also stored a copy of that material, the Commissioner may require the hosting service provider to remove the stored copy to prevent re-posting of the material.

Similar to clause 65, the removal notice would require the provider to remove the cyber-bullying material from the service within 24 hours.

Similar to the appeals mechanisms available for removal notices under clause 65, the AAT can also, on application, review a decision of the Commissioner to give a removal notice under clause 66, or to refuse to give a removal notice (subclauses 220(6) to 220(8) refer).

Clause 67 – Compliance with removal notice

Clause 67 requires a person to comply with a requirement under a removal notice to the extent that the person is capable of doing so. The effect of this provision is that if a person has received a removal notice to remove cyber-bullying material from a service and they have the capacity to remove that material, they must comply with the notice.

This is a civil penalty provision, and 500 penalty units attach to a contravention of this provision. Civil penalty orders are enforceable under Part 4 of the *Regulatory Powers (Standard Provisions) Act 2014* (Regulatory Powers Act), in accordance with subclause 162(1) of the Bill. If a person refuses to comply with a removal notice, daily penalties for contraventions of clause 67 would apply under section 93 of the Regulatory Powers Act.

This penalty unit amount reflects the serious nature of cyber-bullying material directed at an Australian child, and the significant harm and distress that can be caused to a person from being the target of cyber-bullying. In particular, it reflects that the failure to comply with a removal notice can cause significant distress and harm in itself.

It is noted that under the Regulatory Powers Act when determining the amount of the penalty to be imposed, a court is required to consider the nature and extent of the contravention, the loss and damage suffered because of the contravention, the circumstances in which the contravention took place, and whether the person has been found by a court to have engaged in similar conduct in the past. This provides the court with a discretion, in light of the circumstances of the case, to impose a penalty of up to 500 penalty units if the person has been found to be in contravention of this provision.

In addition to the court ordered civil penalty, the Commissioner has access to other enforcement options. Clause 163 provides that this provision is subject to an infringement notice. Clause 164 provides that this provision is subject to an enforceable undertaking. Clause 165 provides that this provision is subject to injunctions.

Clause 68 – Formal warning

Clause 68 enables the Commissioner to issue a formal warning if a person contravenes clause 67.

This is an alternative mechanism available to the Commissioner instead of taking other enforcement action. A formal warning provides a lighter touch mechanism which the Commissioner may choose to use. The Commissioner may issue a formal warning instead of pursuing a civil penalty order or issuing an infringement notice where, for example, it is the first contravention by the person. Whether a formal warning is issued instead of or in addition to taking other enforcement action is a decision for the Commissioner.

Clause 70 – End-user notice

Clause 70 enables the Commissioner to give a written end-user notice to a person who posts cyber-bullying material targeted at an Australian child on a social media service, relevant electronic service or designated internet service.

Clause 70 is directed at an end-user rather than at a provider of a social media service, relevant electronic service, designated internet service, or hosting service provider. This is to allow for circumstances where the end-user is best placed to remove the material, or circumstances where the Commissioner may require more than one party to remove the material, or where the material must be removed from more than one service. For instance, if an end-user has posted cyber-bullying material across several different social media services it may be more efficient to address the removal notice to an end-user for a response.

This clause enables the Commissioner to require a broader range of action than a removal notice under Clauses 65 and 66. An end-user notice may require the end-user to take reasonable steps to remove the material within a specified period, to refrain from posting any cyber-bullying material for which the child is the target and/or to apologise to the subject for posting the material (including in a specified manner and within a specified time).

Subclause 70(2) includes a requirement that the end-user notice must so far as reasonably practicable, identify the particular material to be removed a way that enables the end-user to comply. This is intended to include for example a precise location or description of the material. This is so that the end-user is able to quickly locate, and remove the material in compliance with the notice.

An application may be made to the AAT for review of a decision of the Commissioner to give an end-user notice under clause 70 (subclause 220(10) refers).

Clause 71 – Compliance with end-user notice

Clause 71 requires a person to comply with a requirement under an end-user notice to the extent that the person is capable of doing so. There may be instances where an end-user is unable to prevent cyber-bullying continuing, such as where content has been further disseminated by other parties. In such circumstances, the end-user can only be held responsible for steps that person is capable of undertaking.

This is not a civil penalty provision. The Government does not consider that it would be appropriate to impose a civil penalty because in many cases the perpetrator of cyber-bullying material targeted at a child is also a child.

However, it should be noted that clause 71 is enforceable under Part 7 of the Regulatory Powers Act which creates a framework for using injunctions to enforce provisions (see clause 165).

Clause 72 – Formal warning

Clause 72 allows the Commissioner to issue a formal warning if a person does not comply with an end-user notice.

This is an alternative mechanism available to the Commissioner. A formal warning provides a lighter touch mechanism which the Commissioner may choose to use. The Commissioner might choose to issue a formal warning where, for example, it is the first contravention by the person, or the person is a child. Whether a formal warning is issued instead of or in addition to taking other enforcement action is a decision for the Commissioner.

Clause 73 – Service provider notifications

Clause 73 provides the Commissioner with the power, in certain circumstances, to give the provider of a social media service, relevant electronic service, or a designated internet service a written notice that cyber-bullying material targeted at an Australian child is or has been provided on the service.

This clause provides a formal avenue for the Commissioner to use and enliven the Commissioner's working relationships with service providers. Ordinarily, it is expected that these services would take steps to remove the material once notified, without requiring the Commissioner to give them a removal notice. This may also be the preferred outcome for the complainant, who may be seeking the Commissioner's support to either make a complaint of their behalf, or for support of a complaint the person has already made to the service – for this reason, clause 73 does not require that a complaint has been made to the service provider before the Commissioner may act.

This clause also interacts with Part 4 by alerting the service provider to a possible breach of the service's terms of use and providing the provider with an opportunity to remedy the breach.

Before the Commissioner can give a notification in relation to cyber-bullying material, there must be a complaint made to the Commissioner about the material under clause 30. This means that the Commissioner's power is only enlivened if the victim of the material has complained.

A further condition is that the complainant consents to the notification being given to the provider. This is to allow the victim of the complaint to be aware of and understand the actions being taken by the Commissioner, and that the Commissioner is acting on their behalf.

Subclause 73(2) provides that, if the Commissioner is satisfied there were 2 or more occasions during the previous 12 months on which cyber-bullying material directed at an Australian child was provided on the service, and a complaint was made to the Commissioner and the Commissioner is satisfied that the material contravened that service's terms of use, then the Commissioner may prepare a statement to that effect. The Commissioner may provide a copy of that statement to the provider in question, and, if the Commissioner considers it appropriate to do so, may also publish that statement on the Commissioner's website.

The intention of this section is to introduce a reputational risk for providers and provide them with an incentive to make their services safe for Australian users.

PART 6 – NON-CONSENSUAL SHARING OF INTIMATE IMAGES

DIVISION 1 – Introduction

Part 6 of the Online Safety Bill (the Bill) deals with the treatment of the non-consensual sharing of intimate images.

Clause 74 – Simplified outline of this Part

Clause 74 is a simplified outline of Part 6 of the Bill. This simplified outline is included to assist readers to understand the substantive provisions of Part 6. However, the outline is not intended to be comprehensive. It is intended that readers should rely on the substantive provisions of Part 6.

DIVISION 2 - Intimate images must not be posted without consent etc.

Clause 75 – Posting an intimate image

Clause 75 inserts the prohibition of the non-consensual sharing of intimate images.

Subclause 75(1) provides that a person who is an end-user of a social media service, a relevant electronic service, or a designated internet service, must not post or make a threat to post, an intimate image of another person without their consent. For the prohibition to apply, either the person posting the intimate image, or the person depicted in the image, is to be ordinarily resident in Australia. This link provides an appropriate connection to Australia for the purposes of the Commissioner exercising the Commissioner's powers.

This provision requires that an intimate image be posted rather than simply provided on a service in order to enable a connection to the end-user responsible for posting the material.

This is a civil penalty provision ,and 500 penalty units attach to a contravention of this provision. Civil penalty provisions are enforceable under Part 4 of the Regulatory Powers Act, in accordance with subclause 162(1) of the Bill. This penalty unit amount reflects the serious nature of the non-consensual sharing of intimate images, and the significant harm and distress that can be caused to a person from the sharing of intimate images.

Subclause 75(2) provides that the prohibition does not apply if the person depicted in the intimate image consented to the sharing of the image. This reflects that the targeted behaviour is the sharing of intimate images without the person's consent. If the person consented to the sharing of the intimate image, the prohibition would not be contravened.

There is a note under subclause 75(2) which provides that in proceedings for a civil penalty order against a person, the person who posted or threatened to post the image bears an evidential burden in relation to consent. The effect of this is that if the person is claiming the prohibition did not apply because the person depicted in the image consented to the sharing of the image, the person would be required to provide evidence that consent for the sharing of the image was given.

Subclause 75(3) makes it clear that the prohibition does not apply in relation to an intimate image of a person without attire of religious or cultural significance where the person who

shared the image did not know that the person who is depicted in the image consistently wore that attire whenever the person is in public. This exception is required because, unlike the other definitions of intimate images in subclause 15(2) and 15(3), it may not be clear from the image itself that it is an intimate image. This is because whether the image would be an intimate image will turn on the person's practice in relation wearing of cultural or religious attire in public.

There is a note under subclause 75(3) which provides that in proceedings for a civil penalty order against a person, the person who posted or threatened to post the image bears an evidential burden in relation to showing that the person was not aware that the person depicted in the image consistently wore attire of religious or cultural significance in public. The effect of this is that if the person is claiming the prohibition did not apply because they did not know that the person depicted in the image consistently wore attire of religious or cultural significance in public, the person relying on this exception would be required to provide evidence of the lack of knowledge.

Subclause 75(4) provides that the prohibition does not apply if the posting or threat to post of the intimate image is, or would be, an exempt provision of the intimate image. An exempt provision is defined in clause 86, and provides an exemption to the prohibition in certain circumstances.

There is a note under subclause 75(4) which provides that in proceedings for a civil penalty order against a person, the person who posted or threatened to post the image bears an evidential burden in relation to showing that the sharing of an image was an exempt provision. The effect of this is that if the person is claiming that the prohibition does not apply because the sharing was an exempt provision, the person relying on this exception would be required to provide evidence that the post was in fact an exempt post.

Clause 76 – Formal warning

Clause 76 provides the Commissioner with the discretion to issue a formal warning if a person contravenes the prohibition on the non-consensual sharing of intimate images.

This is a mechanism available to the Commissioner instead of or in addition to taking other enforcement action. A formal warning provides a lighter touch mechanism which the Commissioner may choose to use. The Commissioner may issue a formal warning where, for example, it is the first contravention by the person.

DIVISION 3 – Removal notices

Clause 77 – Removal notice given to the provider of a social media service, relevant electronic service or designated internet service

Clause 77 provides the Commissioner with the power, in certain circumstances, to give the provider of a social media service, relevant electronic service, or designated internet service a removal notice requiring the provider to remove an intimate image that was provided on the service. These notices are given to service providers, as they are considered to be best placed to quickly remove the image from their particular service.

Paragraph 77(1)(b) provides that before the Commissioner can give a removal notice in relation to an intimate image, there must be a complaint made to the Commissioner that the image was shared without consent under clause 32, or an objection notice given to the Commissioner in relation to the image under clause 33. This means that the Commissioner's power is only enlivened if the person depicted in the image, or an authorised person, has complained about, or objected to, the provision of the intimate image.

The Commissioner may issue a removal notice if the Commissioner is satisfied that the person did not consent to the provision of the image and the provision did not constitute an exempt provision (paragraphs 77(1) (c) and 77(1)(d) refer).

The removal notice would require the provider to take all reasonable steps to ensure the removal of the intimate image from the service, and do so within 24 hours (paragraph 77(1)(e) and subparagraph 77(1)(f)(i) refer), or such longer period as the Commissioner allows (subparagraph 77(1)(f)(ii) refers). The period of 24 hours for removal of the notice reflects that the primary concern of the person depicted in the image is often the removal of the image as quickly as possible.

Subclause 77(2) provides that the removal notice must include, as far as is reasonably practicable, enough information for the service provider to be able to identify the intimate image and remove the image in compliance with the notice. This information could be the URL address, or details of the specific site that the intimate image is hosted on, for example. This is to allow the service provider to be able to quickly locate, and remove the intimate image in compliance with the notice.

If the Commissioner was to decide not to issue a removal notice to the service provider, subclause 77(3) would require that the Commissioner give written notice of the refusal to the person who made the complaint, or lodged the objection notice, in relation to the intimate image. It is expected that the Commissioner would also include reasons why the notice was not issued in the circumstances.

The Administrative Appeals Tribunal (AAT) can, on application, review a decision of the Commissioner to give a removal notice under clause 77 (subclause 220(2) refers) and review a decision of the Commissioner to refuse to give a removal notice under clause 77 (subclause 220(4) refers).

Clause 78 – Removal notice given to an end-user

Clause 78 provides the Commissioner with the power, in certain circumstances, to give an end-user a removal notice requiring the person to remove an intimate image that was provided on a social media service, a relevant electronic service, or a designated internet service. The effect of this is that the Commissioner can require the particular person who shared the intimate image to remove the image from the service on which it was posted.

Clause 78 reflects that there are circumstances where the end-user is best placed to remove the intimate images, circumstances where the Commissioner may require more than one party to remove the intimate image, or circumstances where the intimate image must be removed from more than one service. For instance, if an end-user has posted an intimate image across

several different social media services, it may be more efficient to address the removal notice to an end-user for a response.

Similar to clause 77, an end-user is required to take all reasonable steps to remove an intimate image within 24 hours, or such longer period as the Commissioner allows (paragraphs 77(1)(f) and 77(1)(g) refer).

The AAT can, on application, review a decision of the Commissioner to give a removal notice under clause 78 (subclause 220(2) refers) and review a decision of the Commissioner to refuse to give a removal notice under clause 78 (subclause 220(4) refers).

Clause 79 – Removal notice given to a hosting service provider

Clause 79 reflects the same principles and processes as clauses 77 and 78, however, is directed at a hosting service provider rather than at a provider of a social media service, relevant electronic service, designated internet service (under clause 77); or at an end-user (under clause 78). This is to allow for circumstances where the hosting service provider is best placed to remove the intimate image, or circumstances where the Commissioner may require an intimate image to be removed from more than one location. For instance, if an end-user has shared an intimate image onto a service, and a hosting service has also stored a copy of that material, the Commissioner may require the hosting service provider to remove the stored copy to prevent the material being further provided.

The AAT can, on application, review a decision of the Commissioner to give a removal notice under clause 79 (subclause 220 (6) refers) and review a decision to refuse to give a removal notice under clause 79 (subclause 220(8) refers).

Clause 80 – Compliance with removal notice

Clause 80 requires a person to comply with a requirement under a removal notice to the extent that the person is capable of doing so. The effect of this provision is that if a person has received a removal notice to remove an intimate image from a service and they have the capacity to remove that image, they must comply with the notice.

This is a civil penalty provision, and 500 penalty units attach to a contravention of this provision. Civil penalty provisions are enforceable under Part 4 of the Regulatory Powers Act, in accordance with subsection 162(1) of the Bill. If a person refuses to comply with a social media service notice, daily penalties for contraventions of clause 67 would apply under section 93 of the Regulatory Powers Act.

This penalty unit amount reflects the serious nature of non-consensual sharing of intimate images, and the significant harm and distress that can be caused to a person from the sharing of intimate images. In particular, it reflects that the failure to comply with a removal notice can cause significant distress and harm in itself.

It is noted that under the Regulatory Powers Act, when determining the amount of the penalty to be imposed a court is required to consider the nature and extent of the contravention, the loss and damage suffered because of the contravention, the circumstances in which the contravention took place, and whether the person has been found by a court to have engaged in similar conduct in the past. This provides the court with a discretion, in light of the

circumstances of the case, to impose a penalty of up to 500 penalty units if the person has been found to be in contravention of this provision.

In addition to the court ordered civil penalty, the Commissioner has access to other enforcement options. Clause 163 provides that this provision is subject to an infringement notice. Clause 164 provides that this provision is subject to enforceable undertakings. Clause 165 provides that this provision is subject to injunctions.

Clause 81 – Formal warning

Clause 81 provides the Commissioner with the discretion to issue a formal warning if a person does not comply with a removal notice under clauses 77, 78 and 79. In other words, the Commissioner may issue formal warnings to the provider of a social media service, relevant electronic service or designated internet service; to an end-user; and to hosting service providers.

This is an alternative mechanism available to the Commissioner instead of taking other enforcement action. A formal warning provides a lighter touch mechanism which the Commissioner may choose to use. The Commissioner may issue a formal warning instead of pursuing a civil penalty order or issuing an infringement notice where, for example, it is the first contravention by the person, or the person is a child. Whether a formal warning is issued instead of or in addition to taking other enforcement action is at the discretion of the Commissioner.

DIVISION 4 – MISCELLANEOUS

Clause 83 – Remedial direction

Clause 83 provides for the Commissioner to give a person a remedial direction if a person has contravened, or is contravening, the prohibition on the non-consensual sharing of intimate images in clause 75.

Subclause 83(2) provides that the Commissioner may give a person a written direction requiring the person to take specified action directed towards ensuring that the person does not contravene clause 75 in the future. There is a note referring readers to subsection 33(3) of the *Acts Interpretation Act 1901* which makes it clear that this power is to be construed to allow the Commissioner to repeal, rescind, revoke, amend, or vary the direction.

Subclause 83(3) outlines that this is a civil penalty provision, and 500 penalty units attach to a contravention of this provision. Civil penalty provisions are enforceable under Part 4 of the Regulatory Powers Act, in accordance with subclause 162(1) of the Bill. If a person refuses to comply with a social media service notice, daily penalties for contraventions of clause 75 would apply under section 93 of the Regulatory Powers Act.

Subclause 83(4) makes it clear that a direction given to a person under this provision is not a legislative instrument.

The AAT can, on application, review a decision of the Commissioner to give a remedial direction under clause 83 (subclause 220(12) refers).

In addition to a remedial direction, the Commissioner has access to other enforcement options. Clause 163 provides that this provision is subject to an infringement notice. Clause 164 provides that this provision is subject to enforceable undertakings. Clause 165 provides that this provision is subject to injunctions.

Clause 84 – Formal warning

Clause 84 provides the Commissioner with the discretion to issue a formal warning if a person contravenes a remedial direction.

This is a mechanism available to the Commissioner instead of, or in addition to taking other enforcement action. A formal warning provides a lighter touch mechanism which the Commissioner may choose to use. The Commissioner may issue a formal warning where, for example, it is the first contravention by the person.

Clause 85 – Service provider notifications

Clause 85 provides the Commissioner with the power, in certain circumstances, to give the provider of a social media service, relevant electronic service, or designated internet service a written notice that an intimate image is, or has been, provided on the service.

This clause provides a formal avenue for the Commissioner to use the working relationships with service providers. Ordinarily, it is expected that these services would take steps to remove the material once notified, without requiring the Commissioner to give them a removal notice. This may also be the preferred outcome for the complainant, who may be seeking the Commissioner's support to either make a complaint of their behalf, or for support of a complaint the person has already made to the service – for this reason, clause 85 does not require that a complaint has been made to the service provider before the Commissioner may act.

This clause also interacts with Part 4, by alerting the service provider to a possible breach of the service's terms of use and providing the provider with an opportunity to remedy the breach.

Paragraph 85(1)(b) provides that before the Commissioner can give a notification in relation to the non-consensual sharing of intimate images, there must either be a complaint made to the Commissioner about the material under clause 32, or an objection notice given to the Commissioner under clause 33. This means that the Commissioner's power is only enlivened if the person depicted in the intimate image has complained, or an authorised person has complained on behalf of the depicted person to the Commissioner.

A further condition is that the complainant consents to the notification being given to the provider. This is to provide that the complainant is aware of and understands the actions being taken by the Commissioner, and that the Commissioner is acting on their behalf.

Subclause 85(2) provides that, if there were 2 or more occasions during the previous 12 months in which an intimate image was provided on the service, without the consent of the person depicted in the image, and the material contravened that service's terms of use, then the Commissioner may prepare a statement to that effect. The Commissioner may provide a

copy of that statement to the provider in question and, if the Commissioner considers it appropriate to do so, may also publish that statement on the Commissioner's website.

The intention of this section is to introduce a reputational risk for providers and provide them with an incentive to make their services safe for Australian users.

Clause 86 – Exempt provision of an intimate image

Clause 86 inserts a definition of an exempt provision. If an intimate image was provided on a social media service, relevant electronic service, or designated internet service, but the provision of the intimate image is an exempt provision, the prohibition on the non-consensual sharing of an intimate image would not apply, nor would the Commissioner be able to issue a removal notice.

Subclause 86(1) provides that the provision of an intimate image would be an exempt provision if:

- It was necessary for, or of assistance in, enforcing a law of the Commonwealth, State or Territory, or monitoring compliance with or investigating a contravention of a law of the Commonwealth, a State or a Territory (paragraph 86(1)(d) refers). For example, the Commissioner could share an intimate image with the Australian Federal Police who may be investigating whether the sharing of the image amounted to a criminal offence under the *Criminal Code Act 1995* of using a carriage service to menace, harass or cause offence.
- The provision is for the purposes of proceedings in a court or tribunal (paragraph 86(1)(e) refers). For example, if a person applied to the AAT in relation to a decision to issue a removal notice, the Commissioner could electronically provide the Tribunal with the intimate image for the purposes of the review of the decision.
- The provision is for a genuine medical or scientific purpose (paragraph 86(1)(f) refers). For example, an image taken of a child by a doctor to send to a colleague to discuss treatment options, where that image may otherwise amount to an intimate image.
- An ordinary reasonable person would consider the sharing of the image acceptable, having regard to various matters (paragraph 86(1)(g) refers). This is an objective test and the exception means that images that are considered socially acceptable to share, can in fact be shared, notwithstanding they may meet the definition of intimate image. In the case of when an image was posted by an end-user, this test would include the relationship between the end-use of the service and the depicted person. Examples of this include, family photos of small children being bathed by their parents, photographs of models that were specifically taken with permission for advertising or publication, or images that are solely satirical in nature.
- If the intimate image was posted on the service by an end-user who was a protected person (as defined within clause 223), and the posting of the image was in connection with the exercise of a power, or the performance of a function, conferred on the Commissioner under the Bill (paragraph 86(1)(h) refers). For example, an ACMA staff member assisting the Office of the eSafety Commissioner shared an image with another staff member in connection with an investigation into a complaint made regarding the image.

Subclause 86(2) is a power for the Minister to determine, by legislative instrument, one or more conditions which, if satisfied, would mean the post was exempt. This would allow for,

in the future, the Minister to determine that a certain post, or class of posts, were to be exempt posts.

A determination is a legislative instrument for the purposes of the *Legislation Act 2003,* which accordingly must be registered in the Federal Register of Legislation, tabled in the Parliament and would be subject to Parliamentary disallowance.

PART 7 – CYBER-ABUSE MATERIAL TARGETED AT AN AUSTRALIAN ADULT

Part 7 of the Online Safety Bill (the Bill) deals with the treatment of cyber-abuse material targeted at an Australian adult.

DIVISION 1 – Introduction

Clause 87 – Simplified outline of this Part

Clause 87 is a simplified outline of Part 7 of the Bill. This simplified outline is included to assist readers to understand the substantive provisions of Part 7. However, the outline is not intended to be comprehensive. It is intended that readers should rely on the substantive provisions of Part 7.

Clause 88 – Removal notice given to the provider of a social media service, relevant electronic service or designated internet service

Clause 88 provides the Commissioner with the power, in certain circumstances, to give the provider of a social media service, relevant electronic service, or designated internet service a removal notice requiring the provider to remove cyber-abuse material targeted at an Australian adult that is, or has been, provided on the service. The circumstances in which material is provided on a social media service, relevant electronic service or designated internet service are set out in clause 10.

Clause 88 provides for these notices to be given to service providers rather than only to the end-user posting the material, as they are considered to be best placed to ensure quick removal of the material from their particular service and reduce the harm suffered by the target of the cyber-abuse material.

Paragraph 88(1)(b) provides that the Commissioner must be satisfied that the material is cyber-abuse material in accordance with the criteria at clause 7.

Paragraphs 88(1)(c) and 88(1)(d) establish a pre-condition for a removal notice that the complainant had first complained to the service provider, and that the material was not removed from the service within 48 hours or such longer period as the Commissioner allows. This is so that service providers have an opportunity to address any breach of the service's terms of use through its normal processes, prior to any intervention by the Commissioner. Many large service providers facilitate complaints handling as part of their services.

Paragraph 88(1)(e) provides that before the Commissioner can give a removal notice in relation to cyber-abuse material, there must be a complaint made to the Commissioner about the material under clause 36. This is so the Commissioner's power is only enlivened if the target of the material, or another person acting on the target's behalf, has complained about the material.

Paragraph 88(1)(f) provides that a removal notice would require the provider to take all reasonable steps to ensure the removal of the cyber-abuse material from the service, and paragraph 88(1)(g) requires them to do so within 24 hours or such longer period as the Commissioner allows. The period of 24 hours for removal of the material reflects that the

primary concern of the target of the cyber-abuse material is often the removal of the material as quickly as possible.

Subclause 88(2) provides that the removal notice must include, as far as is reasonably practicable, enough information for the service provider to be able to identify and remove the material in compliance with the notice. This information could be the URL address, or details of the specific site that the material is hosted on, for example. This is so that the service provider is able to quickly locate, and remove the material in compliance with the notice.

Subclause 88(3) also provides that if the Commissioner decides not to give a removal notice to the service provider under subclause 88(1), the Commissioner must give written notice of the refusal to the person who made the complaint in relation to cyber-abuse material. It is expected that the Commissioner would also include reasons why the notice was not given in the circumstances.

The AAT can, on application, review a decision of the Commissioner to give a removal notice under clause 88 (subclause 220(2) refers) and review a decision of the Commissioner to refuse to give a removal notice under clause 88 (subclause 220(4) refers).

Clause 89 – Removal notice given to an end-user

Paragraph 89(1)(a) provides the Commissioner with the power, in certain circumstances, to give an end-user a notice requiring the person to remove cyber-abuse material targeted at an Australian adult that was provided on a social media service, a relevant electronic service, or a designated internet service. The effect of this is that the Commissioner can require the particular person who posted the cyber-abuse material to remove the material from the service on which it was provided.

Clause 89 reflects the same principles and processes as clause 88 and clause 90, however is directed at an end-user rather than at a provider of a social media service, relevant electronic service, designated internet service, or hosting service provider. This is to allow for circumstances where the end-user is best placed to remove the material, or circumstances where the Commissioner may require more than one party to remove the material, or where the material must be removed from more than one service. For instance, if an end-user has posted cyber-abuse material across several different social media services, it may be more efficient to address the removal notice to an end-user.

The AAT can, on application, review a decision of the Commissioner to give a removal notice under clause 89 (subclause 220(2) refers) and review a decision of the Commissioner to refuse to give a removal notice under clause 89 (subclause 220(4) refers).

Clause 90 – Removal notice given to a hosting service provider

Clause 90 reflects the same principles and processes as clause 88 and clause 89, however is directed at a hosting service provider rather than at a provider of a social media service, relevant electronic service or designated internet service, or at an end-user. This is to allow for circumstances where the hosting service provider is best placed to remove the material, or circumstances where the Commissioner may require material to be removed from more than one location. For instance, if an end-user has shared cyber-abuse material, and a hosting

service has also stored a copy of that material, the Commissioner may require the hosting service provider to remove the stored copy to prevent re-posting of the material.

The AAT can, on application, review a decision of the Commissioner to give a removal notice under clause 90 (subclause 220(6) refers) and review a decision of the Commissioner to refuse to give a removal notice under clause 90 (subclause 220(8) refers).

Clause 91 – Compliance with removal notice

Clause 91 requires a person to comply with a requirement under a removal notice to the extent that the person is capable of doing so. The effect of this provision is that if a person has received a removal notice to remove cyber-abuse material targeted at an Australian adult from a service and they have the capacity to remove that material or to arrange for its removal, they must comply with the notice.

This is a civil penalty provision, and 500 penalty units attach to a contravention of this provision. Civil penalty provisions are enforceable under Part 4 of the *Regulatory Powers (Standard Provisions) Act 2014* (Regulatory Powers Act), in accordance with subclause 162(1) of the Bill. If a person refuses to comply with a removal notice, daily penalties for contraventions of clause 91 would apply under section 93 of the Regulatory Powers Act.

This penalty reflects the serious nature of cyber-abuse material, and the significant harm and distress that can be caused to a person from being the target or victim of cyber-abuse. In particular, it reflects that the failure to comply with a removal notice can cause significant distress and harm in itself.

In addition to a court-ordered civil penalty, the Commissioner has access to other enforcement options. These enforcement options include infringement notices (clause 163), enforceable undertakings (clause 164) and injunctions (clause 165).

Clause 92 – Formal warning

Clause 92 enables the Commissioner to issue a formal warning if a person contravenes clause 91.

This is an alternative mechanism available to the Commissioner instead of taking other enforcement action. A formal warning provides a lighter touch mechanism which the Commissioner may choose to use. The Commissioner may issue a formal warning instead of pursuing a civil penalty order or issuing an infringement notice where, for example, it is the first contravention by the person, or the person is a child. Whether a formal warning is issued instead of or in addition to taking other enforcement action is a decision for the Commissioner.

Clause 93 – Service provider notifications

Clause 93 provides the Commissioner with the power, in certain circumstances, to give the provider of a social media service, relevant electronic service, or designated internet service a notice that cyber-abuse material targeted at an Australian adult is, or has been, provided on the service.

This clause provides a formal avenue for the Commissioner to use working relationships with service providers. Ordinarily, it is expected that these services would take steps to remove the material once notified, without requiring the Commissioner to give them a removal notice. This may also be the preferred outcome for the complainant, who may be seeking the Commissioner's support to either make a complaint of their behalf, or for support of a complaint the person has already made to the service.

This clause also interacts with the basic online safety expectations at Part 4, by alerting the service provider to a possible breach of the service's terms of use in the view of the Commissioner and providing the provider with an opportunity to remedy the breach.

Paragraph 93(1)(c) provides that before the Commissioner can give a notification in relation to cyber-abuse material, there must be a complaint made to the Commissioner about the material under clause 36. This is so that the Commissioner's power can only be used if the victim of the material has complained.

Subclause 93(1) also provides that the complainant must consent to the notification being given to the provider. This is so that the complainant is aware of and understands the actions being taken by the Commissioner, and understands that the Commissioner is acting on their behalf.

Subclause 93(2) provides that, if there were 2 or more occasions during the previous 12 months on which cyber-abuse material is or has been provided on the service and the material contravened that service's terms of use, then the Commissioner may prepare a statement to that effect. The Commissioner may provide a copy of that statement to the provider in question, and, if the Commissioner considers it appropriate to do so, may also publish that statement on the Commissioner's website.

The intention of this clause is to hold a provider to account for its terms of use, and to uphold the policy principles behind the core expectations at Part 4 – even if the relevant service does not have basic online safety expectations that apply to it. The effect of this section is to introduce a reputational risk for providers and to provide them with incentives to make their services safe for Australian users.

PART 8 – MATERIAL THAT DEPICTS ABHORRENT VIOLENT CONDUCT

Part 8 of the Online Safety Bill (the Bill) provides the Commissioner with new targeted powers to request or require internet service providers (ISPs) to block access to material that promotes, depicts, incites or instructs in abhorrent violent conduct. The intent of this power is to protect the Australian community by preventing viral, that is, the rapid and widespread distribution online, of terrorist and extreme violent material such as the video created by the perpetrator of the March 2019 Christchurch terrorist attack.

The Commissioner's new powers in the Bill are consistent with, and complement, the Commissioner's powers in the *Criminal Code Act 1995* (Criminal Code) enacted by the *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019*. Through the Criminal Code, the Commissioner can issue a notice to advise a content service or hosting service that their service can be used to access abhorrent violent material (AVM). Failure of the provider to ensure the expeditious removal, or cessation of hosting of the material, could subject the provider to a criminal prosecution. Through the Bill, the Commissioner has the power to request or require ISPs to block access to material that promotes, depicts, incites or instructs in abhorrent violent conduct (i.e. terrorist or extreme violent material). Failure to comply with a blocking notice under the Bill can lead to civil penalties.

It is intended that these powers work in tandem with any protocol developed by the Commissioner, in consultation with ISPs and the Communications Alliance (a key industry organisation for the communications industry), that sets out detailed arrangements for how blocking requests and blocking notices will work. The intention is for any such protocol to describe how the Commissioner will provide a blocking request or a blocking notice to an ISP, how affected domain names and the Communications Alliance will be notified, the process for removing blocks and any other detail the Commissioner may deem necessary.

DIVISION 1 – Introduction

Clause 94 – Simplified outline of this Part

Clause 94 is a simplified outline of Part 8 of the Bill. This simplified outline is included to assist readers to understand the substantive provisions of Part 8. However, the outline is not intended to be comprehensive. It is intended that readers should rely on the substantive provisions of Part 8.

DIVISION 2 – Blocking requests

Clause 95 – Blocking request

Clause 95 creates a power for the Commissioner to issue a written request to an ISP to disable access to material that depicts, promotes, incites or instructs in abhorrent violent conduct. The Commissioner must be satisfied that the availability of the material online is likely to cause significant harm to the Australian community. It is not intended for the Commissioner to be able to use this power for material that has limited availability or distribution.

It is anticipated that in the first instance, the Commissioner would issue a voluntary blocking request using the power created by subclause 95(1). ISPs would not be required to respond to a voluntary request, nor would there be any sanctions for non-compliance.

Paragraph 221(2)(f) provides ISPs with protection from civil proceedings when complying with a blocking request from the Commissioner under subclause 95(1).

Subclause 95(1) refers to 'abhorrent violent conduct' which is a defined term for the Bill (see clause 5) as having the same meaning as in Subdivision H of Division 474 of the Criminal Code. The Criminal Code defines abhorrent violent conduct as when a person engages in a terrorist act, murders, attempts to murder, tortures, rapes, or kidnaps another person. The Bill adopts this definition to limit the use of the blocking request power to very seriously harmful material.

Subclause 95(1) refers to 'material that depicts abhorrent violent conduct' which is defined in clause 9 of the Bill as audio, visual, or audio-visual material that records or streams abhorrent violent conduct. This definition is intended to capture live-streamed and recorded video footage, live-streamed and recorded audio recordings (which do not need to be accompanied by visual material), photographs including still images taken from video footage and seriously harmful material such as terrorist manifestos.

The definition of material depicting abhorrent violent conduct is not intended to capture footage of violent sporting events (for example, boxing), medical procedures, or consensual sexual acts that involve elements of violence.

Subclause 95(2) provides examples of steps that the Commissioner may specify in a blocking request to an ISP and include blocking domain names, URLs or IP addresses that provide access to the material.

Subclause 95(3) provides that the Commissioner is not required to observe the requirements of procedural fairness in relation to issuing a blocking request under subclause 95(1). This is intended to exclude any procedural fairness requirements to both an ISP and to any other person to whom procedural fairness might be owed, for example the owner of a website that is being blocked. The reason for excluding procedural fairness in relation to the issuing of the request is to enable the Commissioner to issue a request as quickly as possible to protect the Australian community from seriously harmful material. Exposure to this material has the potential to traumatise and harm those who view it, compound the harm experienced by the victims of such actions, glorify perpetrators, incite further violence and contribute to the radicalisation of end-users.

The blocking request power is limited by subclause 95(4) and subclause 95(5). The Commissioner would need to be satisfied that the availability of the material online is likely to cause significant harm to the Australian community.

In considering whether this is the case, the Commissioner is to have regard to the nature of the material (for example whether it is live streamed material, or particularly high impact material such as a beheading), and the potential for the material to go viral on the internet (i.e. the numbers of end-users who are likely to access the material).

In deciding whether to give the blocking request, the Commissioner must also have regard to whether any other powers conferred on the Commissioner (such as the removal notices for class 1 material under Part 9 or the power under the Criminal Code to notify services of the presence of AVM) could be used to minimise the likelihood that the availability of the

material online could cause significant harm to the Australian community. The intention is that this power be used if this is the most effective mechanism to stop the potential harm to a large number of end-users quickly.

The blocking request power is subject to exemptions in clause 104, for example for material that relates to a news report or current affairs that is in the public interest. These exemptions make sure that the power is sufficiently targeted and is crafted in a way that is reasonable, proportionate and necessary to achieve the policy objective of online safety for Australians.

Clause 96 – Duration of blocking request

Subclause 96(1) highlights that a blocking request remains in force for the period specified in the blocking request, but that the specified period must not be longer than 3 months (subclause 96(2)). Blocking requests are designed to be time-limited to minimise any adverse effects on blocked domains while still achieving the purpose of preventing the harmful proliferation of material that depicts, promotes, incites or instructs in abhorrent violent conduct.

Subclause 96(2) provides the Commissioner with the ability to issue a new blocking request that is in the same, or substantially the same, terms as the original request. The Commissioner has the option to use this power if the material subject to the original request should remain subject to a blocking request but the original request is about to expire. This power allows for the new request to come into force immediately after the expiry of the original request.

Clause 97 – Revocation of blocking request

Clause 97 provides the Commissioner with the power to revoke a blocking request in writing to an ISP. The Commissioner may use this power if the domain or URL ceases to host material subject to the blocking request or if sufficient time has passed to reduce the likelihood of the material reaching a large number of end-users.

Clause 98 – Notification in relation to domain names and URLs

Clause 98 requires the Commissioner to give a copy of the blocking request to the person to whom a domain name is registered (if known) if the blocking request is in force. The Commissioner must provide a copy of the request as soon as practicable after it has been issued to the ISP. The purpose of this clause is to inform owners of affected domains that their services have been blocked.

DIVISION 3 – Blocking notices

Clause 99 – Blocking notice

Subclause 99(1) creates a power for the Commissioner to issue a written notice requiring an ISP to disable access to material that promotes, incites or instructs in abhorrent violent conduct or depicts abhorrent violent conduct. The Commissioner must be satisfied that the availability of the material online is likely to cause significant harm to the Australian community. It is not intended for the Commissioner to be able to use this power for material that has limited availability or distribution.

It is intended that the Commissioner would consider using powers under subclause 99(1) to issue a blocking notice if an ISP does not comply with a voluntary blocking request under subclause 95(1). However, the power is not subject to any precondition or requirement that a blocking request under subclause 95(1) be made first.

Subclause 220(13) provides ISPs with the ability to make an application to the Administrative Appeals Tribunal (AAT) for review of a decision of the Commissioner under clause 99 to give a blocking notice.

Paragraph 221(2)(g) provides ISPs with protection from civil proceedings when complying with a blocking notice from the Commissioner under subclause 99(1).

Subclause 99(2) provides examples of steps that the Commissioner may specify in a blocking notice to an ISP and includes blocking domain names, URLs or IP addresses that provide access to the material.

Subclause 99(3) provides that the Commissioner is not required to observe the requirements of procedural fairness in relation to issuing a blocking notice under subclause 99(1). This is intended to exclude any procedural fairness requirements to both an ISP and to any other person to whom procedural fairness might be owed, for example the owner of a website that is being blocked. The reason for excluding procedural fairness in relation to the issuing of the notice is to enable the Commissioner to issue a notice as quickly as possible to protect the Australian community from seriously harmful material. Exposure to this material can traumatise and harm those who view it, compound the harm experienced by the victims of such actions, glorify perpetrators, incite further violence and contribute to the radicalisation of end-users.

The blocking notice power is limited by subclause 99(4) and subclause 99(5). The Commissioner would need to be satisfied that the availability of the material online is likely to cause significant harm to the Australian community.

In considering whether this is the case, the Commissioner is to have regard to the nature of the material (for example whether it is live streamed material or particularly high impact material such as a beheading), and the potential for the material to go viral on the internet (i.e. the numbers of end-users who are likely to access the material).

In deciding whether to give the blocking request the Commissioner must also have regard to whether any other powers conferred on the Commissioner (such as the removal notices for class 1 material under Part 9 or the AVM notice power under the Criminal Code) could be used to minimise the likelihood that the availability of the material online could cause significant harm to the Australian community. The intention is that this power be used if this is the most effective mechanism to stop the potential harm to a large number of end-users quickly.

The blocking notice power is subject to exemptions in clause 104, for example for material that relates to a news report or current affairs that is in the public interest. These exemptions make sure that the power is sufficiently targeted and is crafted in a way that is reasonable, proportionate and necessary to achieve the policy objective of online safety for Australians.

Clause 100 – Duration of blocking notice

Subclause 100(1) highlights that a blocking notice remains in force for the period specified in the blocking notice but the period specified must not be longer than 3 months (subclause 100(2)). Blocking notices are designed to be time-limited to minimise any adverse effects on blocked domains while still achieving the purpose of preventing the harmful proliferation of material that depicts, promotes, incites or instructs in abhorrent violent conduct.

Subclause 100(3) provides the Commissioner with the ability to issue a new blocking notice that is in the same, or substantially the same, terms as the original notice. The Commissioner has the option to use this power if the material subject to the original notice should remain subject to a blocking notice but the original notice is about to expire. This power allows for the new notice to come into force immediately after the expiry of the original notice.

Clause 101 – Revocation of blocking notice

Clause 101 provides the Commissioner with the power to revoke a blocking notice in writing to an ISP. The Commissioner may use this power if the domain or URL ceases to host material subject to the blocking notice or if sufficient time has passed to reduce the likelihood of the material reaching a large number of end-users.

Clause 102 – Notification in relation to domain names and URLs

Clause 102 requires the Commissioner to give a copy of the blocking notice to the person to whom a domain name is registered (if known) if the blocking notice is in force. The Commissioner must provide a copy of the notice as soon as practicable after it has been issued to the ISP. The purpose of this clause is to inform owners of affected domains that their services have been blocked.

Clause 103 – Compliance with blocking notice

Clause 103 requires a person to comply with a requirement of a blocking notice.

This is a civil penalty provision, and 500 penalty units attach to a contravention of this provision. Civil penalty provisions are enforceable under Part 4 of the *Regulatory Powers (Standard Provisions) Act 2014* (Regulatory Powers Act), in accordance with in accordance with subclause 162(1) of the Bill. If a person refuses to comply with a removal notice, daily penalties for contraventions of clause 99(1) would apply under section 93 of the Regulatory Powers Act.

In addition to the court ordered civil penalty, the Commissioner has access to other enforcement options. Clause 164 provides that this provision is subject to enforceable undertakings. Clause 165 provides that this provision is subject to injunctions. Paragraph 221(2)(g) provides ISPs with protection from civil proceedings when complying with a blocking notice from the Commissioner under subclause 99(1).

DIVISION 4 – Exempt material

Division 4 sets out material that is exempt from a blocking request (subclause 95(1)) or a blocking notice (subclause 99(1)) or from the core basic online safety expectations

(subparagraphs 46(1)(c)(v), (vi), (vii) and (viii) and 46(1)(e)(vi), (vii), (viii) and (ix)). These exemptions act to protect free speech, among other things, and are important limitations on the Commissioner's use of blocking powers.

Clause 104 – Exempt material

Clause 104 sets out exemptions where a blocking request or a blocking notice in subclauses 95(1) and 99(1) or the core basic online safety expectations in subparagraphs 46(1)(c)(v), (vi), (vii) and (viii) and 46(1)(e)(vi), (vii), (viii) and (ix) do not apply.

Each of the exemptions is in relation to the accessibility through an internet carriage service of material that depicts, promotes, incites or instructs in abhorrent violent conduct. The Commissioner's power to issue a blocking request or a blocking notice does not apply if, for example, the accessibility of the material is necessary for law enforcement purposes; court or tribunal processes; scientific, medical, academic or historical research where the access is reasonable in the circumstances for the purpose of that research; or if the material relates to a news report or a current affairs report that is in the public interest, and is made by a professional journalist.

Paragraph 104(1)(a) provides for circumstances where the accessibility of the material is necessary for enforcing a law of the Commonwealth, a State, a Territory, a foreign country or a part of a foreign country. This is intended to avoid situations where a conflict of laws requires the material to both be removed from access by end-users and retained in order to assist law enforcement. Subclause 104(1)(a) resolves this conflict in favour of retaining the material.

Paragraph 104(1)(b) provides for circumstances where the accessibility of the material is necessary for monitoring compliance with, or investigating a contravention of a law of the Commonwealth, a State, a Territory, a foreign country, or part of a foreign country. This is intended to make sure that the offence does not compromise legitimate law enforcement procedures or operations. For example, it may be necessary for a person to maintain access to material that depicts, promotes, incites or instructs in abhorrent violent conduct in a situation where access may assist in identifying the perpetrators of criminal activity.

Paragraph 104(1)(c) provides for circumstances where the accessibility of the material is for the purposes of proceedings in a court or tribunal. This paragraph serves as a constitutional safeguard to make sure that a court or tribunal's access to material is not restricted by the operation of the offence under clause 103(1).

Paragraph 104(1)(d) provides for circumstances where accessibility of the material is necessary for, or of assistance in, conducting scientific, medical, academic or historical research and that accessibility is reasonable in the circumstances for the purpose of conducting that research. For example, this may include where the material is included in academic papers, or where research is being conducted into contemporary reactions to historical case studies of terrorism or other violent events.

Paragraph 104(1)(e) provides for circumstances where the material relates to a news report or a current affairs report, that is in the public interest and is made by a person working in a professional capacity as a journalist. This paragraph is intended to exempt professional journalists from the effect of the offence.

Paragraph 104(1)(f) provides for circumstances where accessibility of the material is in connection with the performance by a public official of that official's duties or functions and the accessibility is reasonable in the circumstances for the purpose of performing those duties or functions. For example, it may be necessary for a public official to maintain access to material that depicts, promotes, incites or instructs in abhorrent violent conduct for security intelligence purposes.

Paragraph 104(1)(g) provides for circumstances where accessibility of the material is in connection with an individual assisting a public official in relation to the performance of public official's duties or functions and the accessibility is reasonable in the circumstances for the purpose of assisting the public official. This could include, for example, where accessibility is in connection with a person assisting a security intelligence officer with the performance of the security intelligence officer's official duties or functions.

Paragraph 104(1)(h) provides for circumstances where accessibility of the material is for the purpose of advocating a lawful procurement of a change to any matter established by law, policy or practice in any Australian jurisdiction or in a foreign country (or part thereof), and the accessibility of the material is reasonable in the circumstances for that purpose. This could include, for example, material published by a civil society body for the purpose of denouncing the laws, policy or practice that enabled the conduct recorded or streamed in that material.

Paragraph 104(1)(i) provides for circumstances where accessibility of the material relates to the development, performance, exhibition or distribution, in good faith, of an artistic work. This could include for example, a still image recording of material that depicts abhorrent violent conduct that is published as part of an online photography exhibition catalogue.

Subclause 104(2) clarifies that for the purposes of clause 104, the definition of public official has the same meaning as in the Criminal Code.

PART 9 – ONLINE CONTENT SCHEME

Part 9 of the Online Safety Bill (the Bill) establishes the online content scheme to provide for the regulation of class 1 and class 2 material (harmful content) on services provided by certain sections of the online industry. The scheme will:

- be based on a model which removes or restricts access to harmful content via the issuing of removal or remedial notices to providers of social media services, relevant electronic services, designated internet services and hosting services (service providers);
- allow the Commissioner to respond to repeated and deliberate failures to comply with notices to remove or restrict class 1 material, by providing an alternative pathway to remove access or restrict access to that content of 'link deletion notices' that may be issued to internet search engine service providers, and 'app removal notices' that may be issued to app distribution service providers;
- enable the Commissioner to have a range of enforcement options against service providers, including civil penalties, formal warnings, infringement notices, enforceable undertakings and injunctions;
- require the Commissioner to make reasonable efforts to ensure that for each section of the online industry, an industry code will be registered within 6 months after the commencement of the Division, or an industry standard will be registered within 12 months after the commencement of the Division; and
- enable the Commissioner to make service provider determinations on rules that are to apply to providers of social media services, relevant electronic services, designated internet services, hosting service providers and internet service providers.

DIVISION 1 – Introduction

Clause 105 – Simplified outline of this Part

Clause 105 is a simplified outline of Part 9 of the Bill. This simplified outline is included to assist readers to understand the substantive provisions of Part 9. However, the outline is not intended to be comprehensive. It is intended that readers should rely on the substantive provisions of Part 9.

Clause 106 – Class 1 material

Clause 106 is an interpretive provision which sets out when online material is class 1 material. For the purposes of the Bill, online material is class 1 material if it is a film (or contents of a film), a publication (or contents of a publication), a computer game, or other material that is neither a film, publication nor computer game, which has been classified or would likely be classified 'Refused Classification' (RC) by the Classification Board under the *Classification (Publications, Films and Computer Games) Act 1995* (Classification Act).

Material considered to be RC is listed in the National Classification Code (May 2005) and the guidelines for the classification of films, computer games and publications. Class 1 material would include material such as child abuse material, child sexual exploitation material, abhorrent violent material, abhorrent sexual activity, advocating a terrorist act (including manifestos) and detailed instruction or promotion in matters of serious crime or violence, the promotion of paedophile activity, descriptions or depictions of child abuse or any other

exploitative or offensive descriptions or depictions involving a person who is, or appears to be, a child under 18 years.

Subclause 106(2) provides that class 1 material includes material that has been classified by an approved classification tool under section 22CF of the Classification Act. Approved classification tools are used by providers of professionally produced content to classify content in accordance with the requirements of the Classification Board.

Clause 107 – Class 2 material

Clause 107 is an interpretive provision which sets out when online material is class 2 material. For the purposes of the Bill, online material is class 2 if it has been, or would likely be, classified in the following way by the Classification Board under the Classification Act:

- a film (or contents of a film) given, or likely to be given, the classification of X 18+ (paragraph (a) and (b));
- a publication (or contents of a publication) given, or likely to be given, the classification of Category 2 restricted (paragraph (c) and (d));
- other material that is neither a film, the contents of a film, publication, the contents of a publication, nor a computer game which if the material were to be classified by the Classification Board in a corresponding way to that of a film, would likely be given the classification of X 18+ (paragraph (e));
- a film (or contents of a film) given, or likely to be given, the classification of R 18+ (paragraphs (f) and (g));
- a publication (or contents of a publication) given, or likely to be given, the classification of Category 1 restricted (paragraphs (h) and (i));
- a computer game given, or likely to be given, the classification of R 18+ (paragraphs (j) and (k)); or
- other material that is neither a film, the contents of a film, publication, the contents of a publication, nor a computer game which if the material were to be classified by the Classification Board in a corresponding way to that of a film would likely be given the classification of R 18+ (paragraph (l)).

Class 2 material covered by paragraph 107(1)(a), (b), (c), (d) or (e) would be mainstream pornography. It would not include material depicting sexual activity that is, for example, abhorrent, which would, if classified by the Classification Board, be classified under the Classification Act as 'RC'.

Class 2 material covered by paragraph 107(1)(f), (g), (h), (i), (j), (k) or (l) would include material depicting violence, implied sexual violence, simulated sexual activity, coarse language, drug use and nudity that is not suitable for audiences under 18 years.

Clause 108 – Restricted access system

Clause 108 allows the Commissioner to declare by written instrument that a specified access-control system or a class of such system is a 'restricted access system' in relation to online material for the purposes of the Bill.

As an aid to interpretation, a note refers to subsection 13(3) of the *Legislation Act 2003* which provides that: if enabling legislation confers on a person the power to make a legislative instrument or notifiable instrument specifying, declaring or prescribing a matter; or doing

anything in relation to a matter; then, in exercising the power, the person may identify the matter by referring to a class or classes of matters.

Subclause 108(3) provides that subclause 108(2) does not limit subsection 33(3A) of the *Acts Interpretation Act 1901* which provides that the instrument making power shall be construed as including a power to make, grant or issue such an instrument with respect to only some of those matters or with respect to a particular class or particular classes of those matters and to make different provision with respect to different matters or different classes of matter.

In making the instrument under subclause 108(1), the Commissioner will be required to have regard to the objective of protecting children from exposure to material that is unsuitable for children, the extent to which the instrument would be likely to result in a financial or administrative burden on providers of social media services, relevant electronic services and designated internet services, or any other relevant matters such as the objects of the Bill.

Once this clause has commenced, the Commissioner will be obliged by subclause 108(5) to ensure a restricted access system declaration is in place at all times.

The purpose of a restricted access system declaration is not to prevent access to age-restricted content (whether it is user-generated content or otherwise) via any platform, but to seek to ensure that:

- access is limited to persons 18 years and over in the case of R 18+ content; and
- that the methods used for limiting this access meet a minimum standard.

This declaration is a legislative instrument for the purposes of the *Legislation Act 2003* which must be registered in the Federal Register of Legislation, tabled in the Parliament and would be subject to Parliamentary disallowance.

DIVISION 2 – Removal notices relating to class 1 material

Clause 109 – Removal notice given to the provider of a social media service, relevant electronic service or designated internet service

Clause 109 provides the Commissioner with the power, in certain circumstances, to give a provider of a social media service, relevant electronic service or designated internet service a notice requiring them to remove class 1 material that is or has been provided on their service.

It is not relevant for the purposes of giving a notice under clause 109 where the service is provided from (i.e. inside or outside Australia); the material just needs to be able to be accessed by end-users in Australia

Paragraph 109(1)(f) requires a provider subject to a notice issued under clause 109 to take all reasonable steps to ensure the removal of the material from the service within 24 hours or a longer period if allowed by the Commissioner. The short timeframe for removal reflects the seriously harmful nature of class 1 material.

To facilitate compliance with a notice under subclause 109(1), subclause 109(2) requires that material be identified in the removal notice in a way that is sufficient to enable a provider to comply with the notice. For example this information could be the URL address, or details of

the specific site that the material is hosted on. This is so that the service provider is able to quickly locate and remove the material in compliance with the notice.

Subclause 220(11) provides that a decision to issue a removal notice is subject to review by the Administrative Appeals Tribunal (AAT).

Clause 110 – Removal notice given to a hosting service provider

Clause 110 provides the Commissioner with the power, in certain circumstances, to give a provider of a hosting service a notice requiring them to cease hosting class 1 material that is hosted by the hosting provider, and that is, or has been, provided on a social media service, relevant electronic service or designated internet service. These notices are given to the hosting service provider, as they are considered to be best placed to prevent access to the material by Australian end-users.

It is not relevant for the purposes of issuing a notice under clause 110 where the material is hosted (i.e. inside or outside Australia); the material just needs to be able to be accessed by end-users in Australia.

Paragraph 110(1)(g) requires a provider subject to a notice issued under clause 110 to take all reasonable steps to cease hosting the material within 24 hours or a longer period if allowed by the Commissioner. The timeframe for removal reflects the seriously harmful nature of class 1 material.

To facilitate compliance with a notice under subclause 110(1), subclause 110(2) requires that material be identified in the removal notice in a way that is sufficient to enable the hosting service provider to comply with the notice.

Subclause 220(11) provides that a decision to issue a removal notice is subject to review by the AAT.

Clause 111 – Compliance with removal notice

Clause 111 requires a person to comply with a requirement under a removal notice to the extent that the person is capable of doing so. The effect of this provision is that if a person has received a notice to remove class 1 material from their service and they are capable of removing that material, or if they have received a notice to cease hosting class 1 material and they are able to cease hosting the material, they must comply with the notice.

Clause 111 provides that a person who contravenes clause 109 or clause 110 will be subject to a maximum penalty of 500 civil penalty units. Civil penalty provisions are enforceable under Part 4 of the *Regulatory Powers (Standard Provisions) Act 2014* (Regulatory Powers Act), in accordance with in accordance with subclause 162(1) of the Bill.

If a person refuses to comply with a notice, the continuing contravention provisions in section 93 of the *Regulatory Powers (Standard Provisions) Act 2014* (Regulatory Powers Act) would apply.

Clause 112 – Formal warning

Clause 112 provides the Commissioner with discretion to issue a formal warning if a person does not comply with a removal notice.

A formal warning provides a lighter touch mechanism which the Commissioner may choose to use. Such a warning may be a precursor to the taking of enforcement action under clauses 163, 164 and 165. Whether a formal warning is issued instead of or in addition to pursuing other options is a decision for the Commissioner.

Clause 113 – Revocation of removal notice

Clause 113 allows the Commissioner to revoke a removal notice in force under clause 109 or clause 110 by written notice.

Clause 113A – Service provider notifications

Clause 113A provides the Commissioner with the power, in certain circumstances, to give the provider of a social media service, relevant electronic service, or designated internet service a notice that class 1 material is, or has been, provided on the service.

This clause provides a formal avenue for the Commissioner to use working relationships with service providers without the need to issue a removal notice.

This clause also interacts with Part 4, by alerting the service provider to a possible breach of the service's terms of use and providing the provider with an opportunity to remedy the breach.

Clause 113A provides that, if there were 2 or more occasions during the previous 12 months on which class 1 material is, or has been, provided on a social media service, relevant electronic service or designated internet service, (other than an exempt Parliamentary content service, an exempt court/tribunal content service, or an exempt official-inquiry content service) and the material can be, or was able to be, accessed by end-users in Australia, and the material contravened that service's terms of use, then the Commissioner may prepare a statement to that effect.

The Commissioner may provide a copy of that statement to the provider in question and, if the Commissioner considers it appropriate to do so, may also publish that statement on the Commissioner's website.

The intention of this clause is to hold a provider to account for its terms of use, and to uphold the policy principles behind the core expectations at Part 4 – even if the relevant service does not have basic online safety expectations that apply to it. The intention of this section is to introduce a reputational risk for providers, to give them incentive to make their services safe for Australian users.

DIVISION 3 – Removal notices relating to class 2 material

Clause 114 – Removal notice given to the provider of a social media service, relevant electronic service or designated internet service

Clause 114 provides the Commissioner with the power, in certain circumstances, to give a provider of a social media service, relevant electronic service or designated internet service a notice requiring them to remove class 2 material covered by paragraph 107(1)(a), (b), (c), (d) or (e) that is, or has been, provided on their service and the material can be accessed by end-users in Australia. These paragraphs cover material that is or would be classified as X 18+ or a Category 2 publication.

Paragraph 114(1)(e) provides that a notice may only be issued to a service provider under clause 114 where the service is provided from Australia. This is intended to capture, for example, social media services who have a registered office or carry on business in Australia or a website based in Australia. It is not intended to capture services based overseas that provide X 18+ material. This type of content is instead intended to be dealt with through industry codes and standards. Failure to comply with a code or standard could result in a civil penalty.

Paragraph 114(1)(g) provides that a provider subject to a notice issued under clause 114 must take all reasonable steps to ensure the removal of the material from their service within 24 hours or a longer period if allowed by the Commissioner. The timeframe for removal reflects the harmful nature of class 2 material, particularly for children.

To facilitate compliance with a notice under subclause 114(1), subclause 114(2) requires that material be identified in the removal notice in a way that is sufficient to enable a provider to comply with the notice.

Subclause 220(11) provides that a decision to issue a removal notice is subject to review by the AAT.

Clause 115 – Removal notice given to a hosting service provider

Clause 115 provides the Commissioner with the power, in certain circumstances, to give a provider of a hosting service a notice requiring the provider to cease hosting class 2 material covered by paragraph 107(1)(a), (b), (c), (d) or (e) that is, or has been, provided on a social media service, relevant electronic service or designated internet service, the hosting provider is hosting the material and the material can be accessed by end-users in Australia. These paragraphs cover material that is or would be classified as X 18+ or a Category 2 publication.

Paragraph 115(1)(f) provides that a notice may only be issued to a hosting service provider under clause 115 where the material is hosted in Australia.

Paragraph 115(1)(h) requires a provider subject to a notice issued under clause 115 to take all reasonable steps to cease hosting the material within 24 hours or a longer period if allowed by the Commissioner. The timeframe for removal reflects the harmful nature of class 2 material, particularly for children.

To facilitate compliance with a notice under subclause 115(1), subclause 115(2) requires that material be identified in the removal notice in a way that is sufficient to enable the hosting service provider to comply with the notice.

Subclause 220(11) provides that a decision to issue a removal notice is subject to review by the AAT.

Clause 116 – Compliance with removal notice

Clause 116 requires a person to comply with a requirement under a removal notice to the extent that the person is capable of doing so.

Clause 116 provides that a person who contravenes clause 114 or clause 115 will be subject to a civil penalty of 500 penalty units. Civil penalty provisions are enforceable under Part 4 of the *Regulatory Powers (Standard Provisions) Act 2014* (Regulatory Powers Act), in accordance with in accordance with subclause 162(1) of the Bill.

If a person refuses to comply with a notice, the continuing contravention provisions in section 93 of the Regulatory Powers Act would apply.

Clause 117 – Formal Warning

Clause 117 provides the Commissioner with discretion to issue a formal warning if a person does not comply with a removal notice. A formal warning provides a lighter touch mechanism which the Commissioner may choose to use. Such a warning may be a precursor to the taking of enforcement action under clauses 163, 164 and 165. Whether a formal warning is issued instead of or in addition to pursuing other options is a decision for the Commissioner.

Clause 118 – Revocation of removal notice

Clause 118 allows the Commissioner to revoke a removal notice in force under clause 114 or clause 115. This is to be by a written notice.

Clause 118A – Service provider notifications

Clause 118A provides the Commissioner with the power, in certain circumstances, to give the provider of a social media service, relevant electronic service, or designated internet service a notice that class 2 material is, or has been, provided on the service.

This clause provides a formal avenue for the Commissioner to use working relationships with service providers without the need to issue a removal notice.

This clause also interacts with Part 4, by alerting the service provider to a possible breach of the service's terms of use and providing the provider with an opportunity to remedy the breach.

Clause 118A provides that, if there were 2 or more occasions during the previous 12 months on which class 2 material covered by paragraph 107(1)(a), (b), (c), (d) and (e) is, or has been, provided on a social media service, relevant electronic service or designated internet service, (other than an exempt Parliamentary content service, an exempt court/tribunal content service,

or an exempt official-inquiry content service) and the material can be, or was able to be, accessed by end-users in Australia, and the material contravened that service's terms of use, then the Commissioner may prepare a statement to that effect.

The Commissioner may provide a copy of that statement to the provider in question and, if the Commissioner considers it appropriate to do so, may also publish that statement on the Commissioner's website.

The intention of this clause is to hold a provider to account for its terms of use, and to uphold the policy principles behind the core expectations at Part 4 – even if the relevant service does not have basic online safety expectations that apply to it. The intention of this section is to introduce a reputational risk for providers, to give them incentive to make their services safe for Australian users.

DIVISION 4 – Remedial notices relating to class 2 material

Clause 119 – Remedial notice given to the provider of a social media service, relevant electronic service or designated internet service

Clause 119 provides the Commissioner with the power, in certain circumstances, to give a provider of a social media service, relevant electronic service or designated internet service a remedial notice. The remedial notice would require the provider to ensure that class 2 material covered by paragraph 107(1)(f), (g), (h), (i), (j), (k) or (l) provided on their service is either removed or subject to a restricted access system. This type of material would be R 18+ or a Category 1 restricted publication. These notices are given to providers of a social media service, relevant electronic service or designated internet service, as they are considered to be best placed to remove the material or ensure the material is subject to a restricted access system.

Paragraph 119(1)(e) provides that a notice may only be issued to a service provider under clause 119 where the service is provided from Australia.

Paragraph 119(1)(g) requires that a provider subject to a notice issued under clause 119 to take all reasonable steps to ensure the material is removed or subject to a restricted access system within 24 hours or a longer period if allowed by the Commissioner. The timeframe for compliance with a notice reflects the harmful nature of class 2 material, particularly for children.

To facilitate compliance with a notice under subclause119(1), subclause 119(2) requires that material be identified in the remedial notice in a way that is sufficient to enable a provider to comply with the notice.

Subclause 220(14) provides that a decision to give a remedial notice is subject to review by the AAT.

Clause 120 – Remedial notice given to a hosting service provider

Clause 120 provides the Commissioner with the power, in certain circumstances, to give a provider of a hosting service a remedial notice. The remedial notice would require the provider to either cease hosting class 2 material covered by paragraph 107(1)(f), (g), (h), (i),

(j), (k) or (l) that is, or has been, provided on a social media service, relevant electronic service or designated internet and is hosted by the hosting provider or ensure that the material is subject to a restricted access system. This type of material would be R 18+ or a Category 1 restricted publication.

Paragraph 120(1)(f) provides that a notice may only be issued to a hosting service provider under clause 120 where the material is hosted in Australia.

Paragraph 120(1)(h) requires a provider subject to a notice issued under clause 120 to take all reasonable steps to ensure the service ceases to host the material or that access to the material is subject to a restricted access system – within 24 hours or a longer period if allowed by the Commissioner. The timeframe for compliance with a notice reflects the harmful nature of class 2 material, particularly for children.

To facilitate compliance with a notice under subclause 120(1), subclause 120(2) requires that material be identified in the remedial notice in a way that is sufficient to enable the hosting service provider to comply with the notice.

Subclause 220(14) provides that a decision to issue a remedial notice is subject to review by the AAT.

Clause 121 – Compliance with remedial notice

Clause 121 requires a person to comply with a requirement under a remedial notice to the extent that the person is capable of doing so. The effect of this provision is that if a person has received a notice to remove or restrict class 2 material covered by paragraph 107(1)(f), (g), (h), (i), (j), (k) or (l) and they have the capacity to remove or restrict that material, or if they have received a notice to either cease hosting class 2 material covered by paragraph 107(1)(f), (g), (h), (i), (j), (k) or (l) or ensure it is subject to a restricted access system and they have the capacity to do so, they must comply with the notice. This type of material would be R 18+ or a Category 1 restricted publication.

Clause 121 provides that a person who contravenes clause 119 or clause 120 will be subject to a civil penalty of up to 500 penalty units. Civil penalty provisions are enforceable under Part 4 of the *Regulatory Powers (Standard Provisions) Act 2014* (Regulatory Powers Act), in accordance with in accordance with subclause 162(1) of the Bill.

If a person refuses to comply with a notice, the continuing contravention provisions under section 93 of the Regulatory Powers Act will apply to the contravention.

Clause 122 – Formal Warning

Clause 122 provides the Commissioner with discretion to issue a formal warning if a person does not comply with a remedial notice. A formal warning provides a lighter touch mechanism which the Commissioner may choose to use. Such a warning may be a precursor to the taking of enforcement action under clauses 163, 164 and 165. Whether a formal warning is issued instead of or in addition to pursuing other options is a decision for the Commissioner.

Clause 123 – Revocation of remedial notice

Clause 123 provides that the Commissioner may revoke a remedial notice in force under clause 119 or clause 120. This is to be by a written notice.

Clause 123A – Service provider notifications

Clause 123A provides that, if there were 2 or more occasions during the previous 12 months on which class 2 material covered by paragraph 107(1)(f), (g), (h), (i), (j), (k) and (l) is, or has been, provided on a social media service, relevant electronic service or designated internet service, the material can be, or was able to be, accessed by end-users in Australia, and the material contravened that service's terms of use, then the Commissioner may prepare a statement to that effect. The Commissioner may provide a copy of that statement to the provider in question and, if the Commissioner considers it appropriate to do so, may also publish that statement on the Commissioner's website.

The intention of this clause is to hold a provider to account for its terms of use, and to uphold the policy principles behind the core expectations at Part 4 – even if the relevant service does not have basic online safety expectations that apply to it. The intention of this section is to introduce a reputational risk for providers, to give them incentive to make their services safe for Australian users.

DIVISION 5 – Link deletion notices

Clause 124 – Link deletion notice

Clause 124 provides the Commissioner with the power, in certain circumstances, to give an internet search engine service provider a link deletion notice requiring the provider to cease providing a link to the class 1 material provided on their service. Paragraph 124(1)(d) requires a provider do so within 24 hours or a longer period if allowed by the Commissioner.

Subclause 124(3) provides that the notice may also require the internet search engine service provider to notify the Commissioner that the provider has ceased to provide a link to the material, and to do so as soon as practicable after the cessation.

Notices issued under clause 124 are given to internet search engine service providers as they play a prominent role in providing Australians with access to online material and can serve as valuable access points to prevent the spread of seriously harmful material.

Recognising that issuing an order to delist a link is a significant power, it is intended that the Commissioner will only issue notices under clause 124 in cases where there has been systemic and repeated posting, hosting or making available of class 1 material and where attempts to remove material at the source have failed. Subclause 124(4) provides that the Commissioner may only issue a link deletion notice where the Commissioner is satisfied that there were 2 or more times during the previous 12 months when end-users in Australia could access class 1 material using a link provided by the service and one or more removal notices issued by the Commissioner under clause 109 or clause 110 were not complied with.

Subclause 220(15) provides that a decision to give a link deletion notice is subject to review by the AAT.

Clause 125 – Compliance with link deletion notice

Clause 125 requires a person to comply with a link deletion notice to the extent that the person is capable of doing so. The effect of this provision is that if a person has received a notice to delist a link and they have the capacity to delist a link, they must comply with the notice.

Clause 125 provides that a person who contravenes clause 124 will be subject to a civil penalty up to 500 penalty units. Civil penalty provisions are enforceable under Part 4 of the *Regulatory Powers (Standard Provisions) Act 2014* (Regulatory Powers Act), in accordance with in accordance with subclause 162(1) of the Bill.

Clause 126 – Formal warning

Clause 126 provides the Commissioner with discretion to issue a formal warning if a person does not comply with a link deletion notice. A formal warning provides a lighter touch mechanism which the Commissioner may choose to use. Such a warning may be a precursor to the taking of enforcement action under clauses 163, 164 and 165. Whether a formal warning is issued instead of or in addition to pursuing other options is a decision for the Commissioner.

Clause 127 – Revocation of link deletion notice

Clause 127 allows the Commissioner to revoke a link deletion notice in force under clause 124. This is to be by a written notice.

DIVISION 6 – App removal notices

Clause 128 – App removal notice

Clause 128 provides the Commissioner with the power, in certain circumstances, to give an app distribution service an app removal notice requiring the provider to cease enabling end-users in Australia to download the app using the service. Paragraph 128(1)(d) requires a provider to do so within 24 hours or a longer period if allowed by the Commissioner.

Subclause 128(3) provides that the notice may require the app distribution service provider to notify the Commissioner that the provider has ceased enabling end-users in Australia to download the app, and to do so as soon as practicable after the cessation.

Notices issued under clause 128 are given to app distribution service providers as they play a prominent role in providing Australians with access to online services and can serve as valuable access points to prevent the spread of seriously harmful material.

Recognising that issuing an order to cease offering an app is a significant power, the Commissioner will only issue notices under clause 128 in cases where there has been systemic and repeated posting of class 1 material on the app and where attempts to remove material at the source have failed. Subclause 128(4) provides that the Commissioner may only issue an app removal notice where the Commissioner is satisfied that there were 2 or more times during the previous 12 months when end-users in Australia could use the service to

download an app that facilitated the posting of class 1 material and one or more removal notices issued by the Commissioner under clause 109 or clause 110 were not complied with.

Subclause 220(16) provides that a decision to issue an app removal notice is subject to review by the AAT.

Clause 129 – Compliance with app removal notice

Clause 129 requires a person to comply with an app removal notice to the extent that the person is capable of doing so. The effect of this provision is that if a person has received a notice to remove an app and they have the capacity to remove the app, they must comply with the notice.

Clause 129 provides that a person who contravenes clause 128 will be subject to a civil penalty of up to 500 penalty units. Civil penalty provisions are enforceable under Part 4 of the *Regulatory Powers (Standard Provisions) Act 2014* (Regulatory Powers Act), in accordance with in accordance with subclause 162(1) of the Bill.

Clause 130 – Formal warning

Clause 130 provides the Commissioner with discretion to issue a formal warning if a person does not comply with an app removal notice. A formal warning provides a lighter touch mechanism which the Commissioner may choose to use. Such a warning may be a precursor to the taking of enforcement action under clauses 163, 164 and 164. Whether a formal warning is issued instead of or in addition to pursing other options is a decision for the Commissioner.

Clause 131 – Revocation of app removal notice

Clause 131 allows the Commissioner to revoke an app removal notice in force under clause 128. This is to be by a written notice.

DIVISION 7 – Industry codes and industry standards

Division 7 sets out rules for the development of self-regulatory industry codes by bodies and associations that represent sections of the online industry. The Commissioner will have the power to make an industry standard (requiring industry compliance) that applies to participants in a particular section of the online industry. The Commissioner may exercise his or her discretion to do so if, for example, he or she considers this is necessary to provide appropriate community safeguards in relation to online safety, or otherwise considers more adequate regulation of a section of the online industry is warranted to achieve the objects of the Act.

Subdivision A – Interpretation

Clause 132 – Industry codes

Clause 132 provides that for the purposes of Division 7, an industry code is a code developed under Division 7, whether or not in response to a request under Division 7.

Clause 133 – Industry standards

Clause 133 defines an industry standard for the purposes of Division 7 as a standard determined under Division 7.

Clause 134 – Online activity

Clause 134 defines an online activity for the purposes of Division 7. An online activity is an activity that consists of: providing a social media service, relevant electronic service, designated internet service, internet search engine service or app distribution service, so far as the service is provided to end-users in Australia; providing a hosting service, so far as the service hosts material in Australia; or providing an internet carriage service, so far as the service is provided to customers in Australia.

Manufacturing, supplying, maintaining or installing equipment that is for use by end-users in Australia of a social media service, relevant electronic service, designated internet service or internet carriage service in connection with the service, is also an online activity for the purposes of Division 7.

These are the activities to which industry codes and industry standards under Division 7 may relate.

Clause 135 – Sections of the online industry

Clause 135 defines sections of the online industry for the purposes of Division 7.

Paragraphs 135(2)(a) to (h) list the groups which are sections of the online industry for the purposes of Division 7. These include groups consisting of providers of social media services, relevant electronic services, designated internet services, internet search engine services, app distribution services, hosting services and internet carriage services and those who manufacture, supply, maintain or install equipment that is for use by end-users in Australia of a social media service, relevant electronic service, designated internet service or internet carriage service in connection with the service.

Such sections of the online industry are identified so that codes will be developed by, and applied to, relevant sections of the industry and requests by the Commissioner (clause 141) for codes may be directed to representatives of relevant sections.

The definition of 'industry sections' is important in ensuring that it is clear for compliance and enforcement purposes to whom a particular code or standard applies. However, it is not intended that the definition of 'industry sections' limit the ability for subsections of the online industry to self-identify and develop their own code.

Clause 136 – Participants in a section of the online industry

Clause 136 provides that, for the purposes of Division 7, a person who is a member of a group that constitutes a section of the online industry is a participant in that section of the online industry. This provision establishes a link between persons and industry sections and is important for compliance and enforcement purposes.

Subdivision B – General principles relating to industry codes and industry standards

Clause 137 – Statement of regulatory policy

Clause 137 is a statement of the Parliament's regulatory policy and provides guidance to the Commissioner in performing functions under Division 7 of Part 9.

Subclause 137(1) provides that it is the Parliament's intention that bodies or associations that the Commissioner is satisfied represent sections of the online industry, should develop codes that are to apply to participants in the respective sections of the industry in relation to their online activities.

Subclause 137(2) provides that it is the Parliament's intention that the Commissioner should make reasonable efforts to ensure that, for each section of the online industry, either an industry code is registered under Division 7 within 6 months after the commencement of the Division or an industry standard is registered under that Division within 12 months after the commencement of the Division. This time period is to allow for the codes or standards to be developed in consultation with interested stakeholders.

Clause 138 – Examples of matters that may be dealt with by industry codes and industry standards

Subclause 138(3) provides examples of matters that may be dealt with by industry codes and industry standards. Subclause 138(3) does not limit the matters that industry codes and industry standards may deal with.

Different online services vary in how they make material available to end-users. The intention of subclause 138(2) is for sections of the online industry to develop industry codes that cover matters most relevant to that sector in terms of regulating end-users' access to class 1 and class 2 material.

Clause 139 – Escalation of complaints

Clause 139 provides that if an industry code or industry standard deals with procedures for dealing with complaints about class 1 or class 2 material on social media services, relevant electronic services or designated internet services, the industry code or industry standard must also deal with the matter of referring complaints about how the complaint is dealt with under the code or standard to the Commissioner.

Subdivision C – Industry codes

Clause 140 – Registration of industry codes

Clause 140 enables a body or association representing a section of the online industry to submit a draft industry code that applies to participants of the section, and deals with one or more matters relating to the online activities of that section, to the Commissioner for registration.

A code submitted under clause 140 should aim to guide industry participants to ensure compliance with their legal obligations and promote the adoption of responsible processes and procedures for dealing with online safety and content issues. It should provide a clear regime to assess and deal with class 1 and class 2 material, fair, efficient and transparent mechanisms for handling public complaints about class 1 and class 2 material, and aim to promote end-user and community confidence in and use of online services.

Subclause 140(2) allows the Commissioner to register an industry code if the requirements set out in subclause 140(1) have been met. These requirements include prior consultation with the Commissioner and the opportunity for public comment.

Subclause 140(4) provides that when a new code is registered under Division 7 and it is expressed to replace another industry code, the other code ceases to be registered.

A decision to refuse to register a code will be reviewable by the AAT on the application of the body or association that developed the code (subclauses 220(17) and 220(18) refer).

Clause 141 – Commissioner may request codes

Clause 141 provides that if the Commissioner is satisfied that a body or association represents a particular section of the online industry, the Commissioner may request them to develop a code that applies to participants of the section and deals with one or more specified matters relating to online activities of those participants.

Subclause 141(2) provides that the Commissioner must specify a period of at least 120 days for a code to be developed and a copy to be given to him or her.

Subclause 141(3) allows the Commissioner to vary the request by extending the period for the code to be given to the Commissioner. Subclause 141(4) provides that subclause 141(3) does not limit the application of subsection 33(3) of the *Acts Interpretation Act 1901*, which provides that where an Act confers a power to make an instrument, the power shall be construed as including a power exercisable in the like manner and subject to the like conditions (if any) to repeal, rescind, revoke, amend, or vary any such instrument.

Subclause 141(5) provides that the Commissioner's notice may specify indicative targets for achieving progress in developing the code.

There are no penalties for not complying with a request to provide a code. However, the industry would be required to comply with any standard determined by the Commissioner under clause 145.

However, this provision does not preclude the Commissioner from determining a standard, under subclause 145, in the first instance, without first requesting the development of an industry code.

Clause 142 – Replacement of industry codes

Clause 142 provides that changes to industry codes are to be achieved by replacement of the code. However, when the changes are of a minor nature, the requirements for consultation with participants in the section and the public in paragraphs 140(1)(e) and (f) will not apply to

the registration process. This will limit consultation to when matters of substance arise and facilitate the making of minor changes to registered codes.

Clause 143 – Compliance with industry codes

Clause 143 provides that, where the Commissioner is satisfied that a participant in a particular section of the online industry has contravened, or is contravening, an industry code registered under Division 7 that applies to them, the Commissioner may direct the participant to comply with the code. The participant must comply with any direction made by the Commissioner.

Subclause 143(2) imposes a civil penalty of 500 penalty units for failure to comply with such a direction. Civil penalty provisions are enforceable under Part 4 of the *Regulatory Powers (Standard Provisions) Act 2014* (Regulatory Powers Act), in accordance with in accordance with subclause 162(1) of the Bill.

The Commissioner's decision to give, vary or refuse to revoke a direction to a person under clause 143 will be reviewable by the AAT on the application of the person concerned (subclauses 220(19) and 220(20)).

Clause 144 – Formal warnings—breach of industry codes

Clause 144 provides that if an industry participant contravenes an industry code, the Commissioner may issue a formal warning to the industry participant. A formal warning provides a lighter touch mechanism which the Commissioner may choose to use. Such a warning may be a precursor to the taking of enforcement action under clauses 163 (infringement notices), 164 (enforceable undertakings) and 165 (injunctions). Whether a formal warning is issued instead of pursuing other options is a decision for the Commissioner.

Subdivision D – Industry standards

Clause 145 – Commissioner may determine an industry standard

Clause 145 enables the Commissioner to make an industry standard that applies to participants in a particular section of the online industry. There does not need to be an attempt by industry to develop an industry code first.

A standard is a legislative instrument for the purposes of the *Legislation Act 2003*, which must be registered on the Federal Register of Legislation and tabled in the Parliament and would be subject to Parliamentary disallowance.

Subclause 145(3) empowers the Minister to give the Commissioner a written direction as to the exercise of the Commissioner's powers under this clause.

This direction is a legislative instrument for the purposes of the *Legislation Act 2003*. However, Ministerial directions are not subject to disallowance, per section 9 of the *Legislation (Exemptions and Other Matters) Regulation 2015.*

Clause 146 – Compliance with industry standards

Clause 146 provides that participants in a particular section of the online industry must comply with any industry standard registered under Division 7 that applies to them.

Clause 146 imposes a civil penalty of 500 penalty units for a contravention of an industry standard. Civil penalty provisions are enforceable under Part 4 of the *Regulatory Powers (Standard Provisions) Act 2014* (Regulatory Powers Act), in accordance with in accordance with subclause 162(1) of the Bill.

Clause 147 – Formal warnings—breach of industry standards

Clause 147 provides that if an industry participant contravenes an industry standard registered under Division 7, the Commissioner may issue a formal warning to the industry participant. A formal warning provides a lighter touch mechanism which the Commissioner may choose to use. Such a warning may be a precursor to the taking of enforcement action under clauses 163 (infringement notices), 164 (enforceable undertakings) and 165 (injunctions). Whether a formal warning is issued instead of pursuing other options is a decision for the Commissioner.

Clause 148 – Public consultation on industry standards

Clause 148 provides that, before the Commissioner determines or varies an industry standard, the Commissioner must make a copy of the draft industry standard available on the Commissioner's website and publish a notice seeking public comment on the draft within the period specified in the notice. Minor variations are exempted from this requirement (subclause 148(3)). The Commissioner must have due regard to any comments made (subclause 148(4)).

Subdivision E – Register of industry codes and industry standards

Clause 149 – Commissioner to maintain Register of industry codes and industry standards

Clause 149 provides for the establishment and maintenance by the Commissioner of a Register of industry codes and standards. The Register must include all industry codes the Commissioner decides to register under Division 7, all industry standards, all requests under clause 141 and directions under clause 143. The Register may be maintained in electronic form and is to be made available for inspection on the Commissioner's website. The maintenance of the Register is intended to provide industry and the public with ready information about the codes and standards that are in force.

Subdivision F – Miscellaneous

Clause 150 – Industry standards prevail over inconsistent industry codes

Clause 150 provides that an industry code registered under Division 7 that is applicable to a person has no effect to the extent to which it is inconsistent with an industry standard that is registered under Division 7 that is applicable to the person. This means that if there is an

industry standard and an industry code applying to the same person, and they were inconsistent, the provisions of the standard would have effect.

DIVISION 8 - Service provider determinations

Clause 151 – Service provider determinations

Clause 151 allows the Commissioner to make a written determination setting out rules that apply to providers of social media services in relation to the provision of social media services, providers of relevant electronic services in relation to the provision of relevant electronic services, providers of designated internet services in relation to the provision of designated internet services, hosting service providers in relation to the provision of hosting services and internet service providers in relation to the supply of internet carriage services.

Determinations made under this clause will be known as 'service provider determinations'. They will be legislative instruments for the purposes of the *Legislation Act 2003* and will be required to be registered on the Federal Register of Legislation and tabled in the Parliament and would be subject to Parliamentary disallowance.

Service provider determinations will have effect only to the extent that they are authorised:

- by paragraph 51(v) (either alone or when read together with paragraph 51(xxxix)) of the Constitution; or
- by section 122 of the Constitution if it would have been authorised by paragraph 51(v) (either alone or when read together with paragraph 51(xxxix)) of the Constitution if section 51 extended to the Territories.

Paragraph 51(v) of the Constitution gives the Parliament the power to make laws with respect to postal, telegraphic, telephonic and other like services. Paragraph 51(xxxix) of the Constitution gives the Parliament the power to make laws with respect to matters incidental to the execution of certain powers vested by the Constitution. Section 122 of the Constitution gives the Parliament the power to make laws in relation to the Territories.

Subclause 151(4) prevents the Commissioner from making a service provider determination unless the determination relates to a matter specified in the legislative rules. The Minister would have the power to make legislative rules under clause 240.

A service provider determination will be able to empower the Commissioner to make decisions of an administrative character (subclause 151(5)).

Subclauses 220(21) and 220(22) provide that administrative decisions of the Commissioner under a service provider determination that relate to a person could be reviewed by the AAT on application of the person concerned.

Clause 152 – Exemptions from service provider determinations

Clause 152 provides that the Minister may determine that a specified provider of social media services, relevant electronic services, designated internet services or hosting services is exempt from all (subclause 152(1)) or specified (subclause 152(2)) service provider determinations. Service provider determinations may be made with respect to a particular class or classes of matters and may make different provision with respect to different matters

or different classes of matters specified individually, in a class, or in any other way (see subsection 33(3A) of the *Acts Interpretation Act 1901*).

A determination made under clause 152 will be able to be unconditional or conditional and will be a legislative instrument for the purposes of the *Legislation Act 2003*. It will be required to be registered on the Federal Register of Legislation and tabled in the Parliament and would be subject to Parliamentary disallowance.

Clause 153 – Compliance with service provider rules

Clause 153 provides that a person must not contravene a service provider rule that applies to them. Clause 153 imposes a civil penalty of 500 penalty units for contravention of a service provider rule. Civil penalty provisions are enforceable under Part 4 of the *Regulatory Powers (Standard Provisions) Act 2014* (Regulatory Powers Act), in accordance with in accordance with subclause 162(1) of the Bill.

Clause 154 – Remedial directions—breach of service provider rules

Clause 154 applies if the Commissioner is satisfied that a provider of a social media service, relevant electronic service, designated internet service, hosting service or internet carriage service has contravened, or is contravening, a service provider rule.

Subclause 154(2) empowers the Commissioner to give the person a written direction requiring that the provider take specified action (including the compliance time for this action) directed towards ensuring that the rule is not contravened, or is not likely to be contravened, in the future.

Subclause 154(3) gives two examples of the kinds of directions which the Commissioner may give under subclause 154(2):

- a direction that the provider implement effective administrative systems for monitoring compliance with a service provider rule; and
- a direction that the provider implement a system designed to inform its employees, agents and contractors of the requirements of a service provider rule.

Subclause 154(4) requires a person to comply with a remedial direction under subclause 154(2) and imposes a civil penalty of 500 penalty units for a contravention of a direction.

If a person refuses to comply with a direction, the continuing contravention provisions in section 93 of the Regulatory Powers Act would apply.

Subclauses 220(21) and 220(22) provide that a decision by the Commissioner to give, vary or refuse to revoke a direction under clause 154 is reviewable by the AAT on the application of the provider concerned.

Clause 155 – Formal warnings—breach of service provider rules

Clause 155 provides that if a person contravenes a service provider rule the Commissioner may issue a formal warning to that person. A formal warning provides a lighter touch mechanism which the Commissioner may choose to use.

DIVISION 9 – Federal Court orders

Clause 156 – Federal Court may order a person to cease providing a social media service

Subclause 156(1) provides that if the Commissioner is satisfied that a social media service has on 2 or more occasions during the previous 12 months contravened a civil penalty provision under Part 9, and as a result of those contraventions it would be a significant community safety risk for the provider to continue providing that social media service in Australia, the Commissioner may apply to the Federal Court for an order that the provider cease providing that service in Australia, as the case requires. This power is intended to be used as a last resort where all other avenues for redress have failed.

Subclause 156(2) provides that if the Federal Court is satisfied, on such an application, that the provider of the social media service has on 2 or more occasions during the previous 12 months contravened a civil penalty provision under Part 9, and as a result of those contraventions it would be a significant community safety risk for the provider to continue providing that service, it will be able to order the provider to cease providing that service in Australia, as the case requires.

Clause 157 – Federal Court may order a person to cease providing a relevant electronic service

Subclause 157(1) provides that if the Commissioner is satisfied that a relevant electronic service has on 2 or more occasions during the previous 12 months contravened a civil penalty provision under Part 9, and as a result of those contraventions it would be a significant community safety risk for the provider to continue providing that relevant electronic service in Australia, the Commissioner may apply to the Federal Court for an order that the provider cease providing that service in Australia, as the case requires. As with clauses 156, 158 and 159, this power is intended to be used as a last resort where all other avenues for redress have failed.

Subclause 157(2) provides that if the Federal Court is satisfied, on such an application, that the provider of the relevant electronic service has on 2 or more occasions during the previous 12 months contravened a civil penalty provision under Part 9, and as a result of those contraventions it would be a significant community safety risk for the provider to continue providing that service, it will be able to order the provider to cease providing that service in Australia, as the case requires.

Clause 158 – Federal Court may order a person to cease providing a designated internet service

Subclause 158(1) provides that if the Commissioner is satisfied that a designated internet service has on 2 or more occasions during the previous 12 months contravened a civil penalty provision under Part 9, and as a result of those contraventions it would be a significant community safety risk for the provider to continue providing that designated internet service in Australia, the Commissioner may apply to the Federal Court for an order that the provider cease providing that service in Australia, as the case requires. As with clauses 156, 157 and 159, this power is intended to be used as a last resort where all other avenues for redress have failed.

Subclause 158(2) provides that if the Federal Court is satisfied, on such an application, that the provider of the designated internet service has on 2 or more occasions during the previous 12 months contravened a civil penalty provision under Part 9 and as a result of those contraventions it would be a significant community safety risk for the provider to continue providing that service, it will be able to order the provider to cease providing that service in Australia, as the case requires.

Clause 159 – Federal Court may order a person to cease supplying an internet carriage service

Subclause 159(1) provides that if the Commissioner is satisfied that a supplier of an internet carriage service has on 2 or more occasions during the previous 12 months contravened a civil penalty provision under Part 9, and as a result of those contraventions it would be a significant community safety risk for the supplier to continue supplying that internet carriage service in Australia, the Commissioner may apply to the Federal Court for an order that the supplier cease supplying that service in Australia, as the case requires. As with clauses 156, 157 and 158, this power is intended to be used as a last resort where all other avenues for redress have failed.

Subclause 159(2) provides that if the Federal Court is satisfied, on such an application, the supplier of an internet carriage service has on 2 or more occasions during the previous 12 months contravened a civil penalty provision under Part 9, and as a result of those contraventions it would be a significant community safety risk for the supplier to continue supplying that service, it will be able to order the supplier to cease supplying that service in Australia, as the case requires.

Examples of civil penalties that would apply to the supplier of an internet carriage service include non-compliance with a relevant industry code (clause 143) or non-compliance with an industry standard (clause 146).

DIVISION 10 – Commissioner may obtain advice from the Classification Board

Clause 160 – Commissioner may obtain advice from the Classification Board

This clause provides that the Commissioner may seek advice from the Classification Board about whether a piece of content is class 1 material, class 2 material covered by paragraph 107(1)(a), (b), (c), (d) or (e) or class 2 material covered by paragraph 107(1)(f), (g), (h), (i), (j), (k) or (l). This option is available to assist the Commissioner when, for example, there may be ambiguity about how to classify a particular piece of material.

The Classification Board may give the advice requested by the Commissioner. However, the advice provided by the Classification Board to the Commissioner under subclause 160(2) does not, by implication, limit the matters that may be taken into account by the Commissioner in forming an independent view about the content and to issue a removal notice.

PART 10 – ENFORCEMENT

Part 10 deals with civil penalty provisions under the Online Safety Bill (the Bill) and applies the civil penalty, infringement notice, enforceable undertaking and injunction frameworks in the *Regulatory Powers (Standard Provisions) Act 2014* (Regulatory Powers Act) to the Bill.

DIVISION 1 – Introduction

Clause 161 – Simplified outline of this Part

Clause 161 is a simplified outline of Part 10 of the Bill. This simplified outline is included to assist readers to understand the substantive provisions of Part 10. However, the outline is not intended to be comprehensive. It is intended that readers should rely on the substantive provisions of Part 10.

Clause 162 – Civil penalty provision

Subclause 162(1) provides for the enforceability of civil penalty provisions in the Bill under Part 4 of the Regulatory Powers Act.

The note to subclause 162(1) provides that Part 4 of the Regulatory Powers Act allows a civil penalty provision to be enforced by obtaining an order for a person to pay a pecuniary penalty for the contravention of the provision.

Subclause 162(2) provides that, for the purposes of Part 4 of the Regulatory Powers Act, the Commissioner is an authorised applicant in relation to a civil penalty provision in the Bill.

Subclause 162(3) provides that, for the purposes of Part 4 of the Regulatory Powers Act, the Federal Court of Australia and the Federal Circuit Court of Australia are the relevant courts in relation to a civil penalty provision in the Bill. While the Federal Circuit Court of Australia is nominated as a relevant court for the purposes of Part 4 of the Regulatory Powers Act, matters in relation to a civil penalty provision in the Bill may be transferred from the Federal Circuit Court of Australia to the Federal Court of Australia, where appropriate.

Subclause 162(4) extends the applicability of Part 4 of the Regulatory Powers Act in relation to a civil penalty provision in the Bill to every external Territory and to acts, omissions, matters and things outside Australia.

Clause 163 – Infringement notices

Clause 163 extends the operation of Part 5 of the Regulatory Powers Act to a contravention of paragraphs 163(1)(a) to (p). Part 5 of that Act creates a framework for using infringement notices in relation to the listed provisions.

Subclause 163(2) provides that a member of the staff of the ACMA who is authorised in writing by the Commissioner is an infringement officer. This is because, under paragraph 182(1), the Commissioner may, by writing, delegate any or all of the Commissioner's functions or powers to a member of the staff of the ACMA. Under Part 5 of the Regulatory Powers Act, an infringement officer may give a person an infringement notice if the officer believes on reasonable grounds that the person has contravened an infringement notice

provision. The Regulatory Powers Act also sets out what matters must be included in the infringement notice.

Where an infringement notice is given, the amount of the infringement notice for a single contravention for an individual would be 12 penalty units and for a body corporate, 60 penalty units.

Subclause 163(3) provides that the Commissioner is the relevant chief executive officer in relation to the provisions under Part 5 of the Regulatory Powers Act in relation to issuing an infringement notice. Under Part 5 of the Regulatory Powers Act, the relevant chief executive is, among other things, able to extend time for payment of an infringement notice, and withdraw an infringement notice.

Under subclause 163(4), the relevant chief executive officer may, in writing, delegate any or all of their powers and functions under Part 5 of the Regulatory Powers Act to a person who is a member of the staff of the ACMA, and is an Senior Executive Service (SES) employee or an acting SES employee. It is considered that SES officers are an appropriate level to which these powers can be delegated, as the seniority of these officers reflects the significant nature of these powers.

There is no provision permitting a delegate to sub-delegate the power, and, accordingly, the standard position in paragraph 34AB(1)(b) of the Acts Interpretation Act applies. That is, a delegate cannot sub-delegate a power or function, unless there is a contrary intention evinced in the legislation.

Subclause 163(5) provides that a delegate must comply with any directions of the relevant chief executive. This reflects that the power being exercised is that of the relevant chief executive, and delegates should exercise the relevant chief executive's powers in accordance with any directions.

Subclause 163(6) makes it clear that Part 5 of the Regulatory Powers Act extends to every external Territory of Australia, and to acts, omissions, matters and things outside of Australia.

Clause 164 – Enforceable undertakings

Subclause 164(1) provides that the provisions of the Bill listed in paragraphs 164(1)(a) to (q) are enforceable under Part 6 of the Regulatory Powers Act. Part 6 of the Regulatory Powers Act creates a framework for accepting and enforcing undertakings in relation to compliance with provisions.

Subclause 164(2) provides that, for the purposes of Part 6 of the Regulatory Powers Act, the Commissioner is an authorised person in relation to the clauses listed in subclause 164(1).

Subclause 164(3) provides that, for the purposes of Part 6 of the Regulatory Powers Act, the Federal Court of Australia and the Federal Circuit Court of Australia are relevant courts in relation to the provisions mentioned in subclause 164(1). While the Federal Circuit Court is nominated as a relevant court in relation to the provisions mentioned in subclause 164(1) for the purposes of Part 6 of the Regulatory Powers Act, such matters may be transferred from the Federal Circuit Court to the Federal Court of Australia, where appropriate.

Subclause 164(4) extends the applicability of Part 6 of the Regulatory Powers Act in relation to the provisions mentioned in subclause 164(1) to every external Territory of Australia and to acts, omissions, matters and things outside Australia.

Clause 165 – Injunctions

Subclause 165(1) provides that the provisions of the Bill listed in paragraphs 165(1)(a) to (s) are enforceable under Part 7 of the Regulatory Powers Act. Part 7 of the Regulatory Powers Act creates a framework for using injunctions to enforce provisions.

Subclause 165(2) provides that, for the purposes of Part 7 of the Regulatory Powers Act, the Commissioner is an authorised person in relation to the provisions mentioned in subclause 165(1) of the Bill.

Subclause 165(3) provides that, for the purposes of Part 7 of the Regulatory Powers Act, the Federal Court of Australia and the Federal Circuit Court of Australia are relevant courts in relation to the provisions mentioned in subclause 165(1) of the Bill.

Subclause 165(4) extends the applicability of Part 7 of the Regulatory Powers Act in relation to the provisions mentioned in subclause 165(1) of the Bill to every external Territory of Australia and to acts, omissions, matters and things outside Australia.

PART 11 – ADMINISTRATIVE PROVISIONS RELATED TO THE COMMISSIONER

Part 11 of the Online Safety Bill (the Bill) deals with the administrative provisions relating to the Commissioner, including appointment of the Commissioner, supplementary powers of the Commissioner, obligations of the Commissioner and the ACMA's obligations to assist the Commissioner.

DIVISION 1 – Introduction

Clause 166 – Simplified outline of this Part

Clause 166 is a simplified outline of Part 11 of the Bill. This simplified outline is included to assist readers to understand the substantive provisions of Part 11. However, the outline is not intended to be comprehensive. It is intended that readers should rely on the substantive provisions of Part 11.

DIVISION 2 – Appointment of the Commissioner

Clause 167 – Appointment of the Commissioner

Subclause 167(1) provides that the Commissioner is to be appointed by the Minister by written instrument.

Subclause 167(2) sets out the eligibility criteria for appointment as the Commissioner. The Minister must be satisfied that a person has substantial experience or knowledge and significant standing in at least one of the fields listed in paragraphs 167(2)(c) to (f). These are:

- the operation of social media services;
- the operation of the internet industry;
- public engagement on issues relating to online safety;
- public policy in relation to the communications sector.

Subclause 167(3) provides that the Commissioner holds office on a full-time basis.

Clause 168 – Period of appointment for the Commissioner

Clause 168 provides that the Commissioner holds office for the period specified in the instrument of appointment (subclause 168(1) refers). This period must not exceed 5 years. The note to clause 168 indicates that the Commissioner may be reappointed as per the *Acts Interpretation Act 1901*.

Clause 169 – Acting appointments

Subclause 169(1) provides that the Minister may appoint a person to act as the Commissioner when there is a vacancy in the office of the Commissioner, or during any period where the Commissioner is absent from duty or Australia, or is unable to perform the duties of the office.

There is a note to subclause 169(1) that refers readers to the rules that apply to acting appointments under section 33A of the *Acts Interpretation Act 1901*.

Subclause 169(2) provides that a person can only act as the Commissioner if they meet the same eligibility requirements for appointment as the Commissioner (see clause 169).

Clause 170 – Application of finance law

Clause 170 provides that for the purposes of the finance law (within the meaning of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act)) the Commissioner is an official of the ACMA.

DIVISION 3 – Terms and conditions for the Commissioner

Clause 171 – Remuneration and allowances

Clause 171 sets out conditions in relation to remuneration and allowances applicable to the Commissioner's appointment.

Subclause 171(1) provides that the Commissioner's remuneration is to be determined by the Remuneration Tribunal. Where no determination by the Remuneration Tribunal is in operation, the Commissioner is to be paid the remuneration that is prescribed by the legislative rules.

Subclause 171(2) provides that the Commissioner is to be paid allowances prescribed by the legislative rules.

Subclause 171(3) provides that clause 171 is subject to the *Remuneration Tribunal Act 1973*.

Clause 172 – Leave of absence

Subclause 172(1) provides that the Commissioner has entitlements to recreation leave as determined by the Remuneration Tribunal.

Subclause 172(2) provides that the Minister may grant the Commissioner leave of absence, other than recreational leave, on terms and conditions determined by the Minister.

Clause 173 – Outside employment

Clause 173 prohibits the Commissioner from engaging in paid employment outside the duties of their office without the Minister's approval.

Clause 174 – Disclosure of interests to the Minister

Clause 174 set outs the Commissioner's disclosure of interest obligations.

Clause 175 – Resignation

Subclause 175(1) provides that the Commissioner may resign the Commissioner's appointment by giving the Minister a written resignation.

Subclause 175(2) provides that the resignation will take effect on the day the Minister receives the written resignation or on a later day specified in the written resignation.

Clause 176 – Termination of appointment

Clause 176 provides the grounds on which the Minister may terminate the Commissioner's appointment.

This standard provision is included to allow the Commissioner to perform the Commissioner's duties without interference, while acknowledging that there may be circumstances where it is both appropriate and warranted for the Commissioner to be replaced as to support the proper function of the office of the Commissioner.

Clause 177 – Other terms and conditions

Clause 177 provides that the Commissioner holds office subject to any further terms and conditions not covered by the Bill that are determined by the Minister.

DIVISION 4 – Other matters

Clause 178 – Supplementary powers

Clause 178 sets out the supplementary powers of the Commissioner.

Subclause 178(1) and subclause 178(2) allow that the Commissioner's powers include the power to enter into contracts on behalf of the Commonwealth.

Subclause 178(3) stipulates that any property held by the Commissioner is held for and on behalf of the Commonwealth. Subclause 178(4) provides that any money received by the Commissioner is received for and on behalf of the Commonwealth.

Subclause 178(5) prohibits the Commissioner from holding real or personal property, or money, on trust for any person other than the Commonwealth. The note to subclause 178(5) states that the Commonwealth may hold real or personal property, or money, on trust.

Subclause 178(6) clarifies that the right to sue is taken not to be personal property for the purposes of subclause 178(3).

Clause 179 – Commissioner's liabilities are Commonwealth liabilities

Subclause 179(1) provides that any of the Commissioner's financial liabilities are to be taken to be liabilities of the Commonwealth.

Subclause 179(2) provides a definition of 'financial liability' for the purposes of clause 179.

Clause 180 – Commissioner has privileges and immunities of the Crown

Clause 180 provides that the Commissioner has the privileges and immunities of the Crown in right of the Commonwealth.

Clause 181 – Delegation by the Commissioner to a member of the staff of the ACMA etc.

Subclause 181(1) provides that the Commissioner may, by writing, delegate any or all of the Commissioner's functions and powers to certain members of the staff of the ACMA or persons whose services are made available to the ACMA under paragraph 55(1)(a) of the ACMA Act.

Subclause 181(2) requires a delegate of the Commissioner to comply with any written directions of the Commissioner.

Subclause 181(3) prohibits the Commissioner from delegating the power to make, vary or revoke a legislative instrument.

Clause 182 – Delegation by the Commissioner to a contractor engaged by the Commissioner

Subclause 182(1) provides that the Commissioner may, by writing, delegate any or all of the Commissioner's functions or powers to a contractor engaged by the Commissioner under subsection 185(1).

Subclause 182(2) requires a delegate to comply with any written directions of the Commissioner.

Subclause 182(3) prohibits the Commissioner from delegating the power to make, vary or revoke a legislative instrument to a contractor delegated powers under this section.

Subclause 182(4) prohibits the Commissioner from delegating certain functions and powers, listed in this subclause, conferred by provisions in the Bill.

The intention behind this provision is that a contractor engaged by the Commissioner under subclause 185(1) cannot be delegated any of the Commissioner's powers or functions where there are civil penalties attached, or where, for example, it would be more appropriate for the Commissioner or APS staff, who are subject to the *Public Service Act 1999*, to exercise the power. The contractor could, for example, be involved in day-to-day work to inform the decisions of the Commissioner; however, final decision-making authority will rest with the Commissioner personally, or a sufficiently senior APS employee who has had the appropriate functions and powers delegated to them under clause 181. It is not intended that this provision extends to general delegations under the *PGPA Act* or *Public Service Act 1999*. For example, a contractor engaged by the Commissioner under subclause 185(1) could not sign a contract on behalf of the Commonwealth. However, the contractor could undertake work to inform a contract up to the point of signature.

Subclause 182(5) prohibits the Commissioner from delegating a function or power conferred by the *Regulatory Powers (Standard Provisions) Act 2014* (Regulatory Powers Act).

Clause 183 – Annual report

Clause 183 requires the Commissioner to prepare and give to the Minister, for presentation to the Parliament, an annual report as soon as practicable after the end of each financial year on

the operations of the Commissioner during that year. The note to clause 183 refers to additional rules about annual reports in section 34C of the *Acts Interpretation Act 1901*.

Clause 184 – Assistance to the Commissioner

Clause 184 requires the ACMA to assist the Commissioner to perform their functions and exercise their powers, including providing advice and making resources and facilities available to the extent that the Commissioner reasonably requires (subclauses 184(1) and 184(2)).

Subclause 184(3) requires the ACMA to make available members of their staff to assist the Commissioner, to the extent reasonably required by the Commissioner, to perform the Commissioner's functions and powers, so long as the Commissioner considers that these staff have the skills, qualifications or experience necessary to assist the Commissioner.

Subclause 184(4) provides that, when performing services for the Commissioner, these staff are subject to direction by the Commissioner.

Subclause 184(5) enables the Minister, by legislative instrument, to give directions to the ACMA in relation to the performance or exercise of its functions or powers under clause 184 (i.e. in relation to providing assistance to the Commissioner). The notes to subclause 184(5) refer to the power to vary and revoke instruments under subsection 33(3) of the *Acts Interpretation Act 1901* and regulations made under the *Legislation Act 2003* which provide that the disallowance and sunsetting arrangements under that Act do not apply to such a direction.

Subclause 184(6) provides that the ACMA must comply with a direction made under subclause 184(5). The effect of this is that staff provided to the Commissioner by the ACMA are accountable to the Commissioner in the performance of their duties under the Bill and act independently of the ACMA in making decisions under this Bill.

This Bill does not displace the existing common law duty of employees to comply with lawful and reasonable directions by the employer, or the existing duty of APS employees to comply with a lawful and reasonable direction under the APS Code of Conduct as set out in section 13 of the *Public Service Act 1999*.

In the rare event that a conflict should arise between a direction from the Commissioner and from the Chair, member or associate member of the ACMA, it is intended that staff comply with the directions of the Commissioner to the extent that the direction relates to giving effect to the exercise of the Commissioner's statutory functions and powers.

Subclause 184(7) provides that, for the purpose of clause 184, a member of the staff of the ACMA includes an officer or employee whose services are made available to the ACMA under paragraph 55(1)(a) of the *Australian Communications and Media Authority Act 2005* (the ACMA Act).

Clause 185 – Contractors engaged by the Commissioner

Subclause 185(1) enables the Commissioner, on behalf of the Commonwealth, to engage contract staff to assist the Commissioner to perform their functions and powers.

Subclause 185(2) provides that contract staff are to be engaged on the terms and conditions that the Commissioner determines in writing.

Subclause 185(3) provides that contract staff engaged under subclause 185(1) are subject to the directions of the Commissioner. Subclause 185(3) reflects the same principles as subclause 184(4), however, applies to contractors rather than staff of the ACMA.

Clause 186 – Commissioner not subject to direction by the ACMA

Clause 186 makes it clear that the Commissioner is not subject to direction by the ACMA, any of its members or associate members, or any member of its staff in relation to the performance of a function, or the exercise of a power, by the Commissioner.

Clause 187 – Consultants

Subclause 187(1) enables the Commissioner, on behalf of the Commonwealth, to engage consultants that have suitable qualifications and experience. Subclause 187(2) stipulates that consultants are to be engaged on the terms and conditions that the Commissioner determines in writing.

Clause 188 – Minister may give directions to the Commissioner

Subclause 188(1) enables the Minister, by legislative instrument, to give directions to the Commissioner about the performance of the Commissioner's functions or exercise of the Commissioner's powers. The notes to subclause 188(1) refer to the power to vary and revoke instruments under subsection 33(3) of the *Acts Interpretation Act 1901* and section 42 and Part 4 of Chapter 3 of the *Legislation Act 2003* which provide that the disallowance and sunsetting arrangements under that Act do not apply.

Subclause 188(2) provides that directions made under subclause 188(1) must be of a general nature only.

The Commissioner is required to comply with a direction made under subclause 188(1) (subclause 188(3)).

PART 12 – ONLINE SAFETY SPECIAL ACCOUNT

Part 12 of the Online Safety Bill (the Bill) continues the existence of the Online Safety Special Account (Special Account) and provides for how moneys may be credited to, or debited from, the Special Account.

Clause 189 – Simplified outline of this Part

Clause 189 is a simplified outline of Part 12 of the Bill. This simplified outline is included to assist readers to understand the substantive provisions of Part 12. However, the outline is not intended to be comprehensive. It is intended that readers should rely on the substantive provisions of Part 12.

Clause 190 – Online Safety Special Account

Subclause 190(1) continues the existence of the Special Account.

Subclause 190(2) provides that the Special Account is a special account for purposes of the PGPA Act.

Subclause 190(3) provides that the ACMA is to administer the Special Account.
Subclause 190(4) stipulates that an amount must not be debited from the Special Account without the Commissioner's written approval. In giving written approval, the Commissioner must comply with the requirements of the PGPA Act. The *Public Governance, Performance and Accountability Act 2013* (PGPA Act) sets out the way in which officials must handle public money, public property and other resources of the Commonwealth.

The Special Account sits within the ACMA's portfolio budget statements, however, it is accounted for as its own item.

Clause 191 – Credits to the Account

Clause 191 provides for the crediting of money to the Special Account.

Subclause 191(1) enables the Minister to determine that a specified amount be credited to the Special Account. If there is an appropriation for a departmental item that relates to the ACMA in an Appropriation Act, the Minister may, by writing, determine that a specified amount be debited against that appropriation and credited to the Special Account.

Subclause 191(2) provides that a determination made under subclause 191(1) is a legislative instrument, but is not subject to Parliamentary disallowance under section 42 of the *Legislation Act 2003*. Exclusion from disallowance is appropriate in this instance to provide certainty of funding to the Commissioner.

Subclause 191(3) provides that, for the purposes of the application of clause 191 to an Appropriation Act, the term 'ACMA departmental item' is defined to mean a departmental item (within the meaning of the Appropriation Act) that relates to the ACMA.

Clause 192 – Purposes of the Account

Clause 192 sets out the purposes of the Special Account, which are:

- to enhance online safety for Australians;
- to make grants under paragraph 27(1)(g);
- to pay remuneration and other employment-related costs and expenses in respect of APS employees whose duties relate to the performance or exercise of the Commissioner's functions or powers; and
- to pay any other costs, expenses and other obligations incurred by the Commonwealth in connection with the performance or exercise of the Commissioner's functions or powers.

The note to clause 192 draws the reader's attention to section 80 of the PGPA Act, which deals generally with special accounts.

PART 13 – INFORMATION GATHERING POWERS

Part 13 of the Online Safety Bill (the Bill) deals with arrangements for the exercise of the Commissioner's information-gathering powers. The intention is that Part 13 will operate to support the Commissioner's investigations under the Bill, such as investigations under clauses 31, 34, 37 and 42.

The Commissioner would have the power to obtain information about the identity or contact details of an end-user of a social media service, relevant electronic service or designated internet service, from the provider of that service, where the Commissioner believes on reasonable grounds that the identity information or contact details are relevant to the operation of the Bill.

A person must comply with a requirement under a written notice from the Commissioner to provide this information within a period and in a manner and form specified in the notice, to the extent that the person is capable of doing so.

If the social media service, relevant electronic service, or designated internet service fails to comply with the requirements in the notice, they will be subject to a civil penalty.

Clause 193 – Simplified outline of this Part

Clause 193 is a simplified outline of Part 13 of the Bill. This simplified outline is included to assist readers to understand the substantive provisions of Part 13. However, the outline is not intended to be comprehensive. It is intended that readers should rely on the substantive provisions of Part 13.

Clause 194 – Commissioner may obtain end-user identity information or contact details

Subclause 194(1) sets out the scope of the Commissioner's power to obtain information about the identity and contact details of an end-user from a social media service, relevant electronic service or designated internet service.

Before the Commissioner may exercise this power, the Commissioner must believe on reasonable grounds that the person providing the service has information about the identity or contact details of the end-user. For instance, the Commissioner could form this belief if the service ordinarily collects identity information about an end-user at the time of account creation, or for the purpose of financial transactions with that service or a third party while using that service, or for account recovery purposes. This disclosure of personal information to the Commissioner by the provider would be in connection with the purpose for which it was collected and would be consistent with the permissible secondary purpose exemption for disclosure under Australian Privacy Principle 6.

Before exercising the power, the Commissioner must also believe on reasonable grounds that the identity information or contact details are relevant to the operation of the Bill. While end-users expect privacy online, this provision is intended to unmask anonymity where the Commissioner has reasonable grounds to believe that an end-user's identity or contact details are relevant to the operation of the Bill. For example, the Commissioner may require this information to give an end-user notice under clause 70, to a person who posts cyber-bullying material targeted at an Australian child on a social media service, relevant electronic service

or designated internet service. This provision is reasonable, necessary and proportionate to achieving the aim of administering the operation of the Bill.

Subclause 194(2) provides that the Commissioner may issue a notice that requires the person providing the service to give the Commissioner the identity or contact information of the end-user within the period of time, and in the manner and form specified in the notice.

Clause 195 – Compliance with notice

Clause 195 provides that a person must comply with a notice issued under subclause 194(2) to the extent that they are capable of doing so.

This is a civil penalty provision, with a penalty of 100 penalty units attached to a contravention of this provision. Civil penalty provisions are enforceable under Part 4 of the *Regulatory Powers (Standard Provisions) Act 2014* (Regulatory Powers Act), in accordance with clause 162 of the Bill.

It is noted that under the Regulatory Powers Act, when determining the amount of the penalty to be imposed, a court is required to consider the nature and extent of the contravention, the nature and extent of any loss or damage suffered because of the contravention, the circumstances in which the contravention took place, and whether the person has been found by a court to have engaged in similar conduct in the past. This provides the court with a discretion, in light of the circumstances of the case, to impose a penalty of up to 100 penalty units if the person has been found to be in contravention of this provision.

In addition to the court ordered civil penalty, the Commissioner has access to other enforcement options. Clause 165 provides that this provision is subject to injunctions.

Clause 196 – Self-incrimination

Subclause 196(1) provides that a person is not excused from complying with a requirement under clause 194 by claiming that the information or contact details might incriminate them.

Subclause 196(2) provides that compliance with a requirement under clause 194 may not be used as evidence in a civil proceeding for the recovery of a penalty (other than proceedings for the recovery of a penalty under clause 195); or in criminal proceedings against the person (other than proceedings for an offence against section 137.1 or 137.2 of the Criminal Code that relates to this Part). Sections 137.1 and 137.2 of the Criminal Code include offences about the production of false or misleading information or documents.

Subclause 196(2) enables the person to comply with a requirement under clause 194 without that compliance being used against them in another civil or criminal matter. The purpose of the subclause is to facilitate the provision of identity information or contact details about an end-user where the Commissioner believes on reasonable grounds that the information is, or the contact details are, relevant to the operation of the Bill.

Subclause 196(3) provides that an individual is not excused from complying with a requirement under clause 194 by claiming the privilege against self-exposure to a penalty (other than a penalty for an offence).

PART 14 – INVESTIGATIVE POWERS

Part 14 of the Online Safety Bill (the Bill) deals with arrangements for the exercise of the Commissioner's investigative powers.

For the purposes of an investigation, the Commissioner will have the power to require the attendance of a person, the production of documents and the answering of questions relevant to the subject matter of the investigation. These powers would be used where the Commissioner considers it the best way to conduct an investigation in accordance with the Bill, and would be expected to be used in a way that is reasonable and proportionate including by requiring examination records to be kept and shared with the person examined.

Clause 197 – Simplified outline of this Part

Clause 197 is a simplified outline of Part 14 of the Bill. This simplified outline is included to assist readers to understand the substantive provisions of Part 14. However, the outline is not intended to be comprehensive. It is intended that readers should rely on the substantive provisions of Part 14.

Clause 198 – Application of this Part

Clause 198 makes clear that Part 14 applies to an investigation being conducted by the Commissioner under clauses 31, 34, 37 or 42. That is, an investigation in response to a complaint made about cyber-bullying material targeted at an Australian child under clause 30; a complaint made about non-consensual sharing of intimate images made under clause 32; a complaint made about cyber-abuse material targeted at an Australian adult under clause 36; a complaint made about class 1 material or class 2 material under clause 38; a complaint relating to breach of a service provider rule under clause 39; or a complaint relating to breach of an industry code or industry standard under clause 40. Part 14 also applies to an investigation conducted by the Commissioner under clause 42 on the Commissioner's own initiative.

Clause 199 – Notice requiring appearance for examination

Clause 199 provides that, for the purposes of an investigation being conducted by the Commissioner, the Commissioner may, by written notice, summon a person to attend before the Commissioner or a delegate of the Commissioner specified in the notice. The notice could include a requirement for the person to produce documents or answer questions, or provide documents or other information relevant to the subject matter of the investigation.

For the purposes of an investigation, the Commissioner may summon an end-user as well as a representative of a service provider.

Clause 200 – Examination on oath or affirmation

Clause 200 is a standard provision relating to the examination of a person under an oath or affirmation.

Clause 201 – Examination to take place in private

Clause 201 stipulates that the examination of a person during an investigation under this Bill must be conducted in private. Clause 201 allows that person to have an adviser present at such an examination. An adviser could include a legal adviser.

Clause 202 – Record to be made of examination

Clause 202 requires that any examination of a person under this Bill be recorded, and gives that person a right to be given a copy of that record.

Clause 203 – Production of documents for inspection

Clause 203 allows the Commissioner to require a person to give the Commissioner or the Commissioner's delegate access to documents relevant to an investigation, and allows the Commissioner or the Commissioner's delegate to make copies of any of those documents.

Clause 204 – Protection of persons giving evidence

Clause 204 is a standard clause affording protection to persons giving evidence or producing documents at an investigation.

Clause 205 – Non-compliance with requirement to give evidence

Subclause 205(1) makes it an offence for a person required to answer questions, give evidence or produce documents under this Part, to refuse or fail to take the oath or make the affirmation when required; refuse or fail to answer a question that the person is required to answer; or refuse or fail to produce a document that the person is required to produce. Subclause 205(2) provides that this is also a civil penalty provision.

Imprisonment for 12 months (subclause 205(1)), and 100 penalty units (subclause 205(2)), attach to a contravention of these provisions. Civil penalty provisions are enforceable under Part 4 of the *Regulatory Powers (Standard Provisions) Act 2014* (Regulatory Powers Act), in accordance with clause 162 of the Act. If a person refuses to comply with a requirement, daily penalties for contraventions of subclause 205(2) would apply under section 93 of the Regulatory Powers Act. It is noted that under the Regulatory Powers Act, when determining the pecuniary penalty to be imposed, a court is required to consider the nature and extent of the contravention, the nature and extent of any loss or damage suffered because of the contravention, the circumstances in which the contravention took place, and whether the person has been found by a court to have engaged in similar conduct in the past. This provides the court with a discretion, in light of the circumstances of the case, to impose a penalty of up to 100 penalty units if the person has been found to be in contravention of this provision.

There are exemptions from the requirements to provide evidence.

Subclause 205(3) provides that subclause 205(1) and subclause 205(2) do not apply if the person has a reasonable excuse for non-compliance. Subclause 205(4) provides for an exemption on the grounds that answering the question or production of the document would self-incriminate a person. There are notes to the effect that the defendant would bear an evidential burden in relation to these matters, which is consistent with the provisions of the

Regulatory Powers Act and subsection 13.3(3) of the Criminal Code in respect of civil and criminal matters in which a defendant seeks to rely on an exemption or excuse provision.

Subclause 205(5) provides an exemption in the circumstance where the person is a journalist and the answer to the question or production of the document would disclose the identity of a confidential source.

PART 15 – DISCLOSURE OF INFORMATION

Part 15 of the Online Safety Bill (the Bill) sets out the circumstances in which the Commissioner may disclose information, and the parties to which such information may be disclosed, including among others: the Minister, an ACMA staff member, Royal Commissions, specified regulators and law enforcement agencies, teachers, school principals and parents or guardians.

Clause 206 – Simplified outline of this Part

Clause 206 is a simplified outline of Part 15 of the Bill. This simplified outline is included to assist readers to understand the substantive provisions of Part 15. However, the outline is not intended to be comprehensive. It is intended that readers should rely on the substantive provisions of Part 15.

The note to clause 206 cross-references clause 224 (which provides for referral of maters to law enforcement agencies).

Clause 207 – Scope

Clause 207 sets out the scope of Part 15, which applies to information obtained by the Commissioner through the performance of functions, or exercise of powers conferred on the Commissioner by the Bill.

Disclosures of such information are only authorised in the particular instances dealt with expressly in Part 15. In addition, any personal information collected by the Commissioner would be appropriately dealt with in accordance with the *Privacy Act 1988*, regardless of whether this collection occurred due to the Commissioner performing functions, or exercising powers conferred on the Commissioner by the Bill.

Clause 208 – Disclosure to Minister

Clause 208 provides for the Commissioner to disclose information to the Minister. The Minister is the Minister administering the Bill.

Clause 209 – Disclosure to Secretary, or APS employees, for advising the Minister

Clause 209 provides for the Commissioner to disclose information to the Secretary or an APS employee in the Department who has been authorised, by the Secretary in writing, to receive the information.

Clause 210 – Disclosure to a member of the staff of the ACMA etc.

Paragraph 210(a) allows the Commissioner to disclose information to a member of the staff of the ACMA.

Paragraph 210(b) allows the Commissioner to disclose information to an officer or employee whose services are made available to the ACMA under paragraph 55(1)(a) of the *Australian Communications and Media Authority Act 2005*. Under paragraph 55(1)(a), the ACMA may make an arrangement with an ‘authority of the Commonwealth’ for the services of officers or

employees of the authority to be made available for the purposes of the ACMA. An 'authority of the Commonwealth' means a Commonwealth entity or a Commonwealth company for the purposes of the *Public Governance, Performance and Accountability Act 2013*, or any other body established for a public purpose by or under a law of the Commonwealth.

Paragraph 210(c) allows the Commissioner to disclose information to a person engaged under subclause 185(1) of the Bill. For the purposes of subclause 185(1), the Commissioner may engage persons on behalf of the Commonwealth, to assist the Commissioner to perform the Commissioner's functions and exercise the Commissioner's powers.

Paragraph 210(d) allows the Commissioner to disclose information to a consultant engaged by the Commissioner on behalf of the Commonwealth under clause 187 of the Bill.

Any disclosures under clause 210 of the Bill are to be for purposes relating to the performance of the Commissioner's functions or the exercise of the Commissioner's powers.

Clause 211 – Disclosure to Royal Commissions

Clause 211 allows the Commissioner to disclose information to a Royal Commission, and to impose conditions in relation to such information.

Subclause 211(1) provides for the Commissioner to disclose information to a Royal Commission.

Subclause 211(2) allows the Commissioner to impose written conditions to be complied with in relation to information which has been disclosed to a Royal Commission. This is a safeguard by which the Commissioner may limit further disclosure, where it is appropriate to do so.

Subclause 211(3) provides that an instrument under subclause 211(2) that imposes conditions relating to one particular disclosure is not a legislative instrument. Subclause 211(3) is declaratory of the law and is included to assist readers rather than create an exception to the *Legislation Act 2003*.

Subclause 211(4) provides that any other instrument under subclause 211(2) is a legislative instrument.

This means that if the written conditions are in relation to a particular disclosure, then the document in which the written conditions appear is not a legislative instrument. If the conditions are meant to be more broad ranging and apply to multiple disclosures (e.g. all disclosures made to a particular Royal Commission) then the document containing the conditions is a legislative instrument.

Clause 212 – Disclosure to certain authorities

Subclause 212(1) provides for the Commissioner to disclose information that will enable or assist an authority listed in paragraphs 212(1)(a) to 212(1)(i), to perform or exercise any of the authority's function or powers. The listed authorities include the ACMA, the National Children's Commissioner, the Office of the Australian Information Commissioner, the Secretary of the Department administered by the Minister administering the *Classification (Publications, Films and Computer Games) Act 1995* or an APS employee in the Department

whose duties relate to that Act, the Australian Federal Police (AFP), the Commonwealth Director of Public Prosecutions, or an authority of a State or Territory responsible for enforcing one or more laws of the State or Territory. For example, the Commissioner might disclose information to the AFP under paragraph 212(1)(e) if satisfied that the information would assist the AFP to investigate an offence under the Criminal Code.

Paragraph 212(1)(h) and paragraph 212(1)(i) allows the Commissioner to disclose information obtained in the performance of a function or exercise of a power conferred on the Commissioner by or under the Bill, to an authority of a foreign country that is responsible for regulating matters or enforcing laws of that country relating to either or both the capacity of individuals to use social media services, relevant electronic services and designated internet services in a safe manner, or material that is accessible to, or delivered to, end-users of social media services, relevant electronic services and designated internet services. For example, the Commissioner may disclose information to the United States Department of Justice or the Commissioner's counterpart (i.e. Online Safety Commissioner) in another country.

The disclosures authorised under clause 212 are not intended to reduce the capacity for the Commissioner to make other authorised disclosures, such as the referral of matters to law enforcement agencies under clause 224 of the Bill.

Subclause 212(2) allows the Commissioner to impose written conditions to be complied with in relation to information disclosed under subclause 212(1). This provides a safeguard by which the Commissioner may limit further disclosure of the information, where it is appropriate to do so.

Subclause 212(3) provides that an instrument under subclause 212(2) that imposes conditions relating to one particular disclosure is not a legislative instrument. Subclause 212(3) is declaratory of the law and is included to assist readers rather than create an exception to the *Legislation Act 2003*.

Subclause 212(4) provides that any other instrument under subclause 212(2) is a legislative instrument.

This means that if the written conditions are in relation to a particular disclosure, then the document in which the written conditions appear is not a legislative instrument. If the conditions are meant to be more broad ranging and apply to multiple disclosures (e.g. all disclosures made to particular authorities) then the document containing the conditions is a legislative instrument.

Clause 213 – Disclosure to teachers or school principals

Under subclause 213(1), the Commissioner may disclose information to a teacher or school principal if satisfied that the information will assist in the resolution of a complaint about cyber-bullying of a child made under clause 30 of the Bill. For example, where cyber-bullying involves a group of school students, enlisting the help of the school or schools attended by the students may be the quickest and most effective means of resolving the complaint. The Commissioner will need to be able to disclose information to the teacher or school principal in these circumstances.

Subclause 213(2) allows the Commissioner to impose written conditions to be complied with in relation to information disclosed under subclause 213(1). For example, the Commissioner may impose a condition preventing secondary disclosures to third parties.

Subclause 213(3) provides that an instrument under subclause 213(2) that imposes conditions relating to one particular disclosure is not a legislative instrument. Subclause 213(3) is declaratory of the law and is included to assist readers rather than create an exception to the *Legislation Act 2003*.

Subclause 213(4) provides that any other instrument under subclause 213(2) imposing conditions is a legislative instrument.

This means that if the written conditions are in relation to a particular disclosure, then the document in which the written conditions appear is not a legislative instrument. If the conditions are meant to be more broad ranging and apply to multiple disclosures (e.g. all disclosures made to teachers) then the document containing the conditions is a legislative instrument.

Clause 214 – Disclosure to parents or guardians

Subclause 214(1) enables the Commissioner to disclose information to a parent or guardian of an Australian child if the Commissioner is satisfied that the information will assist in the resolution of a complaint made under clause 30 of the Bill. This is intended to assist in the resolution of complaints about cyber-bullying material targeted at an Australian child.

Subclause 214(2) allows the Commissioner to impose written conditions to be complied with in relation to information disclosed under subclause 214(1). Such conditions may include a requirement preventing secondary disclosures to third parties.

Subclause 214(3) provides that an instrument under subclause 214(2) that imposes conditions relating to one particular disclosure is not a legislative instrument. Subclause 214(3) is declaratory of the law and is included to assist readers rather than create an exception to the *Legislation Act 2003*.

Subclause 214(4) provides that any other instrument under subclause 214(2) imposing conditions is a legislative instrument.

This means that if the written conditions are in relation to a particular disclosure, then the document in which the written conditions appear is not a legislative instrument. If the conditions are meant to be more broad ranging and apply to multiple disclosures (e.g. all disclosures made to parents or guardians) then the document containing the conditions is a legislative instrument.

Clause 215 – Disclosure with consent

Clause 215 allows the Commissioner to disclose information that relates to the affairs of a person if the person has consented to the disclosure and the disclosure is in accordance with that consent. An example of where the Commissioner might disclose information that relates to the affairs of a person with their consent is to issue a service provider notification about the provision of cyber-abuse material targeted at an Australian adult on a service under clause 93.

Clause 216 – Disclosure of publicly available information

Clause 216 allows the Commissioner to disclose information that is already publicly available.

Clause 217 – Disclosure of summaries and statistics

Clause 217 allows the Commissioner to disclose summaries of de-identified information and statistics derived from de-identified information. As defined in clause 5 of the Bill, information is de-identified if the information is no longer about an identifiable individual or an individual who is reasonably identifiable. This clause is required to support the Commissioner in preparing summaries and statistics about online safety. One of the functions of the Commission is to collect, analyse, interpret and disseminate information related so online safety (paragraph 27(1)(d)).

Clause 218 – Relationship with Parts 13 and 15 of the *Telecommunications Act 1997*

Clause 218 clarifies that the disclosures authorised by Part 15 of the Bill do not authorise a disclosure of information that is prohibited by Parts 13 and 15 of the *Telecommunications Act 1997* (Telecommunications Act). Part 13 of the Telecommunications Act regulates the use and disclosure of protected information obtained by certain bodies during the supply of telecommunication services. Part 15 of the Telecommunications Act sets out arrangements for certain designated communications providers to provide assistance to law enforcement and security agencies.

PART 16 – MISCELLANEOUS

Part 16 of the Online Safety Bill (the Bill) deals with miscellaneous matters, such as review of decisions and legislative rules.

Clause 219 – Simplified outline of this Part

Clause 219 is a simplified outline of Part 16 of the Bill. This simplified outline is included to assist readers to understand the substantive provisions of Part 16. However, the outline is not intended to be comprehensive. It is intended that readers should rely on the substantive provisions of Part 16.

Clause 220 – Review of decisions

Clause 220 provides for the review, by the Administrative Appeals Tribunal (AAT), of certain decisions made by the Commissioner, and sets out who may make an application for such review. The AAT serves an important function in conducting independent merits review of administrative decisions made under Commonwealth laws, providing a fresh look at decisions that may impact on persons, including providers of a social media service, relevant electronic service, designated internet service and end-users of those services, as well as providers of a hosting service, internet carriage service or bodies or associations representing sections of the online industry. The decisions that are reviewable, and who can make an application to the AAT, are covered in subclause 220(1) to subclause 220(22), outlined below. 'Internet carriage service', 'social media service', 'relevant electronic service', 'designated internet service' and 'hosting service' are defined terms for the purposes of the Bill (see clauses 5, 13, 14 and 17).

Subclause 220(1) allows applications to be made to the AAT for a review of a decision of the Commissioner under clauses 49 or 56 to give a notice to a provider of a social media service, a relevant electronic service or a designated internet service to prepare a report about compliance with the basic online safety expectations.

Subclause 220(2) allows applications to be made to the AAT for a review of a decision of the Commissioner under clauses 65, 77, 78, 88 or 89 to give a removal notice to a provider of a social media service, a relevant electronic service or a designated internet service.

Subclause 220(3) limits who can make an application under subclause 220(2) to the provider of the social media service, relevant electronic service or designated internet service who received a notice under clauses 65, 77, 78, 88 or 89 or, if the material was posted by an end-user of the service, the end-user who posted the material that is the subject of the notice, as these are the parties directly affected by the notice.

Under subclause 220(4), applications may be made to the AAT to review decisions made by the Commissioner to refuse to give a removal notice under clauses 65, 77, 78, 88 or 89 to a social media service, a relevant electronic service or a designated internet service.

Subclause 220(5) limits who can make an application to the AAT under subclause 220(4) to a person who made a complaint under clauses 30, 32, or 36 about material posted on a particular social media service, a relevant electronic service or a designated internet service, or a person who has been given consent by the person who was or is the target of material that

was posted on a social media service, relevant electronic service or designated internet service.

A decision by the Commissioner to give a removal notice to a hosting service provider under clauses 66, 79 or 90 is reviewable under subclause 220(6).

Subclause 220(7) limits who can make an application under subclause 220(6) to the hosting service provider to which the decision of the Commissioner under clause 66, 79 or 90 results in that provider being given a removal notice, or where the material was posted on the service by an end-user, the end-user who posted the material that is the subject of the notice under clauses 66, 79 or 90.

Subclause 220(8) allows for applications for review to be made to the AAT regarding a decision by the Commissioner under clauses 66, 79 or 90 to refuse to give a removal notice to a hosting service provider about material hosted by the provider.

Subclause 220(9) limits who can make an application for review under subclause 220(8) to a person who made a complaint under clauses 30, 32 or 36. In the case of a refusal to give a notice under clause 66 or clause 90, an application may also be made by, or with the consent of, the person who was the target of the material. In the case of a refusal to give a removal notice under clause 79 relating to an intimate image of a person, the application may be made by, or with the consent of, that person.

Subclauses 220(10) to 220(16) provide for an application to be made to the AAT to review certain decisions of the Commissioner, and do not provide limitations on who can make an application for review. This is in contrast with previous subclauses in clause 220 which limited the ability to apply to the AAT to persons directly affected by a decision.

Subclause 220(10) allows for applications to be made to the AAT for a review of a decision by the Commissioner under clause 70 to give an end-user notice relating to cyber-bullying material targeted at an Australian child.

Subclause 220(11) provides for an application to be made to the AAT for a review of a decision by the Commissioner under clauses 109, 110, 114 or 115 to give a removal notice to a provider of a social media service, a relevant electronic service, a designated internet service or a hosting service in relation to class 1 material or class 2 material.

Subclause 220(12) allows for applications for review of decisions under clause 83 to give a remedial direction requiring a person to take a specified action directed towards ensuring the person does not contravene the prohibition on posting an intimate image without consent under clause 75.

Subclause 220(13) provides for applications to be made to the AAT for review of a decision under clause 99 to give a blocking notice to an internet service provider (ISP), in relation to material that depicts, promotes, incites or instructs in abhorrent violent conduct, that can be accessed using an internet carriage service supplied by the ISP.

Subclause 220(14) allows for applications for review of a decision under clauses 119 or 120 to give a remedial notice relating to class 2 material to a social media service, relevant electronic service, designated internet service or hosting service provider.

Subclause 220(15) allows for an application for review of a decision under clause 124 to give a link deletion notice to a provider of an internet search engine service.

Subclause 220(16), allows for an application for review of a decision to give an app removal notice under clause 128 to a provider of an app distribution service.

Subclause 220(17), allows for an application to be made for a review of a decision of the Commissioner to refuse to register an industry code under clause 140.

Subclause 220(18) limits who can make an application for review under subclause 220(17) to the body or association that developed the industry code.

Under subclause 220(19), an application can be made to the AAT for a review of a decision of the Commissioner under clause 143 (compliance with industry codes) to give a direction to a person, vary a direction that is applicable to a person, or refuse to revoke a direction that is applicable to a person.

Subclause 220(20) limits who can make an application for a review under subclause 220(19) to a person who has been subject of a decision of the Commissioner to give a direction, vary a direction or refuse to revoke a direction.

Paragraph 220(21)(a) allows for an application to be made to the AAT for a review of a decision made by the Commissioner regarding service provider determinations under subclause 151(5). This relates to decisions made empowering the Commissioner to make decisions of an administrative character.

Applications made for review under paragraph 220(21)(b) are limited to decisions made by the Commissioner under clause 154 to give a direction to a person, vary a direction that is applicable to a person or refuse to revoke a direction that is applicable to a person.

Subclause 220(22) limits who can make an application under subclause 220(21) to a person directly concerned with the Commissioner's decision to issue a direction, a variance to a direction or a refusal to revoke a direction.

Clause 221 – Protection from civil proceedings

Clause 221 provides for instances in which a person is protected from civil proceedings in relation to certain acts done under the Bill. The intention is that a person, such as a complainant or end-user, or a social media service, relevant electronic service or ISP, should not face financial liability to other persons for certain actions taken in good faith under the Bill.

Subclause 221(1) prohibits civil proceedings from being brought against a person in respect of loss, damage or injury of any kind suffered by another person because of any acts done in good faith as listed in paragraphs 221(1)(a) to (j). This includes acts such as making a complaint about cyber-bullying, adult cyber-abuse, the non-consensual sharing of intimate images or class 1 material or class 2 material provided on a social media, relevant electronic or designated internet service.

Subclause 221(2) prohibits civil proceedings from being brought against a person in respect of acts done in compliance with the types of notices set out in paragraphs 221(2)(a) to 221(2)(h).

Clause 222 – Liability for damages

Persons listed in paragraphs (a) to (b) of clause 222 are not liable to an action or other proceeding for damages for, or in relation to, an act or matter done or omitted to be done in good faith in:

- the performance or purported performance of any function; or
- in the exercise or purported exercise of any power;

that is conferred on the Commissioner by or under the Bill.

Clause 223 – Protection from criminal proceedings—Commissioner, Classification Board etc.

The purpose of clause 223 is to protect from criminal proceedings those persons listed whose powers and functions require them to do things in relation to material which would otherwise be prohibited. This provision is necessary to enable the protected persons to effectively perform their statutory functions. A list of protected persons is set out in paragraphs 223(1)(a) to 223(1)(h).

Clause 223 provides protection from criminal liability for 'protected persons' (defined in subclause 223(1)) in relation to any of the acts listed in subclause 223(2) that were undertaken in connection with the exercise of a power, or the performance of a function, conferred on the Commissioner or the Classification Board by or under the Bill. This is intended to protect those delegated persons and body corporate entities who have undertaken activities as per subclause 223(2) in connection with exercise of a power or performance of a function conferred to them by the Bill.

For the purposes of clause 223, 'possession of material' as referred to in paragraph 223(2)(b) includes the custody or control of material, as clarified under subclause 223(3).

Clause 224 – Referral of matters to law enforcement agencies

Clause 224 provides that the Commissioner must notify law enforcement agencies of particular material provided on a social media service, relevant electronic service or designated internet service if the Commissioner becomes aware of the particular material (through performance of a function or exercise of a power conferred by or under the Bill), and is satisfied that it is of a sufficiently serious nature to warrant such referral. In those circumstances, the Commissioner must notify the material to a member of an Australian police force (defined in clause 5), or another person or body if there is an arrangement between the Commissioner and the chief (however described) of an Australian police force under which the Commissioner is authorised to notify the material to that other person or body (subclause 224(1)(c) and 224(1)(d)).

Subclause 224(2) provides that the manner in which material is to be notified under paragraph 224(1)(d) to a member of an Australian police force (as defined in clause 5 to

include the AFP and the police force of a State of Territory) includes, but is not limited to, a manner ascertained in accordance with an arrangement between the Commissioner and the chief (however described) of the police force concerned.

Subclause 224(3) allows for the member of an Australian police force that has been notified of the particular material under clause 224 to notify the material to a member of another law enforcement agency.

Subclause 224(4) provides that clause 224 does not, by implication, restrict the Commissioner's power to refer other matters to a member of an Australian police force. The Commissioner may choose, for example, to refer matters to a member of the Australian police force through powers vested in clause 212.

Clause 225 – Deferral of action in order to avoid prejudicing a criminal investigation

In certain cases, it is possible that a police investigation may be concurrent with a complaint to the Commissioner about particular material. As a safeguard, clause 225 provides that if a member of an Australian police force (as defined in clause 5) satisfies the Commissioner that taking an action under the Bill in relation to material provided on a social media service, relevant electronic service or designated internet service would prejudice a criminal investigation, the Commissioner may defer taking that action until the end of a particular period of the criminal investigation for which the complaint about the particular material relates.

Clause 226 – Copies of material

Clause 226 allows the Commissioner to make copies of material for the purposes of an investigation of a complaint under the clauses listed in paragraph 226(1)(a), a consideration under clause 35, or a request under clause 160 for advice from the Classification Board.

Subclause 226(2) exempts the Commissioner from any copyright infringement if the Commissioner chooses to make copies of material under subclause (1).

Clause 227 – Compensation for acquisition of property

Clause 227 establishes a compensatory regime for acquisition of property under the Bill, or a legislative instrument made under the Bill. Subclause 227(1) sets out that the Commonwealth is liable to pay a reasonable amount of compensation if, within the meaning of paragraph 51(xxxi) of the Constitution, property was acquired from a person otherwise than on just terms (within the meaning of paragraph 51(xxxi) of the Constitution).

Subclause 227(2) provides that if there is no agreement reached on the amount of compensation, then the person may commence proceedings in the Federal Court or the Supreme Court of a State or Territory for reasonable compensation as determined by the court.

Clause 228 – Service of notices by electronic means

Clause 228 provides that paragraphs 9(1)(d) and 9(2)(d) of the *Electronic Transactions Act 1999* do not apply to a notice under the Bill or the *Regulatory Powers (Standard Provisions)*

Act 2014, so far as that Act relates to the Bill. Paragraphs 9(1)(d) and 9(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, and are not considered appropriate in circumstances where the Commissioner may frequently have access to electronic contact details only.

Clause 229 – Service of notices on contact person etc.

Clause 229 is a deeming provision setting out when a summons, process or notice is taken to have been served on, or given to, a provider of a social media service, relevant electronic service, designated internet service, hosting service, internet search engine service, app distribution service or internet service, or to a body corporate incorporated outside Australia.

Subclause 229(1) provides that this clause applies to the summons or processes outlined in paragraphs (a) to (b), and a notice outlined in paragraphs (c) to (d).

Subclause 229(2) provides that if a summons, process or notice is required to be served on the provider of a social media service, relevant electronic service, designated internet service, hosting service, internet search engine service, app distribution service or internet service; and there is an individual who has been designated by the provider as their employee or agent and contact person for the purpose of the Act; and that person's contact details have been provided to the Commissioner; the summons, process or notice is deemed to have been served on the provider if it served on or given to that contact person.

Subclause 229(3) provides that if a summons, process or notice is required to be served on, or given to a body corporate that is incorporated outside Australia, does not have a registered or principal office in Australia, and has an agent in Australia, the summons, process or notice deemed to be served on, or given to, the agent of the body corporate in Australia if it is served on that agent.

Subclause 229(4) clarifies that subclauses 229(2) and 229(3) have effect in addition to section 28A of the *Acts Interpretation Act 1901* which deals with the service of documents.

Clause 230 – Instruments under this Act may provide for matters by reference to other instruments

Subclause 230(1) provides that an instrument made under the Bill may make provision in relation to a matter by applying, adopting or incorporating (with or without modifications) provisions of any Act as in force at a particular time, or as in force from time to time.

Subclause 230(2) provides that an instrument made under the Bill may make a provision in relation to a matter by applying, adopting or incorporating (with or without modifications) matters contained in any other instrument or writing as in force or existing at a particular time, or as in force or existing from time to time, even if the other instrument or writing does not yet exist when the instrument under this Bill is made.

Subclause 230(3) provides that references to any other instrument or writing in subsection (2) to an instrument or writing made by a person or body in Australia or elsewhere, whether of legislative or administrative or other nature and whether or not that instrument or writing has

any legal force or effect. For example, it is envisaged that an instrument under the Bill may adopt an international technical standard or performance indicator.

Subclause 230(4) is an interpretive provision that does not limit the generality of clause 230 or its contents.

Subclause 230(5) provides that subclauses 230(1) and 230(2) have effect regardless of anything in the *Acts Interpretation Act 1901* or the *Legislation Act 2003*.

Clause 231 – This Act does not limit Schedule 8 to the *Broadcasting Services Act 1992*

Clause 231 clarifies that the Bill does not limit the operation of Schedule 8 to the *Broadcasting Services Act 1992* (BSA). Schedule 8 of the BSA confers power on the ACMA to make rules about gambling promotional content provided on an online content service in conjunction with a live sporting event, and to give remedial directions to online content service providers that contravene specified rules.

Clause 232 – This Act does not limit the *Telecommunications Act 1997*

Clause 232 clarifies that the Bill does not limit the operation of the *Telecommunications Act 1997*.

Clause 233 – Implied freedom of political communication

Clause 233 is a constitutional safeguard, which provides that the Bill does not apply to the extent (if any) that it would infringe any constitutional doctrine of implied freedom of political communication.

Subclause 233(2) provides that subclause 233(1) does not limit the application of section 15A of the *Acts Interpretation Act 1901* to the Bill. This subclause outlines that every Act shall be read and construed subject to the Constitution.

Clause 234 – Concurrent operation of State and Territory laws

In accordance with clause 234, it is the intention of Parliament that the Bill does not apply to the exclusion of a law of a State or Territory, to the extent to which that law is capable of operating concurrently with the Bill.

Clause 234 is intended to allow different Commonwealth and State or Territory laws that address aspects of cyber-bullying, for example, to operate concurrently with one another.

Clause 235 – Liability of Australian hosting service providers and internet service providers under State and Territory laws etc.

Clause 235(1) provides that the law of a State or Territory, or a rule of common law or equity has no effect to the extent to which it:

- subjects or would have the direct or indirect effect of subjecting an Australian hosting service provider or an internet service provider to liability (whether civil or criminal) in respect of hosting or carrying particular online content, where the provider was not aware of the nature of the content; or

- requires or would have the direct or indirect effect of requiring an Australian hosting service provider or internet service provider to monitor, make inquiries about, or keep records about online content hosted or carried by the provider.

The Minister is provided with the power by subclause 235(2) to make a legislative instrument to exempt a specified law of a State or Territory, or a specified rule of common law or equity from operation of subclause 235(1).

Subclause 235(3) provides that this exemption may be unconditional or subject to such conditions (if any) as are specified in the instrument.

An exemption is a legislative instrument for the purposes of the *Legislation Act 2003* which must be registered in the Federal Register of Legislation, tabled in the Parliament and would be subject to Parliamentary disallowance.

Subclause 235(4) provides that the Minister may declare that a specified law of a State or Territory, or a specified rule of common law or equity, has no effect to the extent to which the law or rule has a specified effect in relation to an Australian hosting service provider. Subclause 235(5) performs the same function as subclause 235(4), but in relation to a law or rule that has a specified effect in relation to an ISP.

Subclause 235(6) is a constitutional safeguard. It provides that a declaration under subclause 235(4) or 235(5) has effect only to the extent that it is authorised by paragraph 51(v) of the Constitution (either alone or when read together with paragraph 51(xxxix) of the Constitution), or is authorised by section 122 of the Constitution and would have been authorised by paragraph 51(v) of the Constitution (either alone or when read together with paragraph 51(xxxix) of the Constitution) if section 51 of the Constitution extended to the Territories.

Clause 236 – This Act not to affect performance of State or Territory functions

Clause 236 is also a constitutional safeguard. It provides that a power conferred by this Bill must not be exercised in such a way as to prevent the exercise of the powers, or the performance of the functions, of government of a State, the Northern Territory or the Australian Capital Territory.

Clause 237 – Revocation or variation of instruments

Subsection 33(3) of the *Acts Interpretation Act 1901* provides that where an Act confers a power to make, grant or issue any instrument of a legislative or administrative character, the power shall be construed as including a power exercisable in the like manner and subject to the like conditions (if any) to, relevantly, revoke or vary any such instrument.

Various clauses of the Bill permit the making of instruments of this nature, and expressly provide for the revocation and variation of instruments so made. Clause 237 provides that a provision of the Bill that expressly authorises the revocation or variation of an instrument does not, by implication, limit the application of subsection 33(3) of the *Acts Interpretation Act 1901* in relation to other instruments under this Act.

This clause operates to put beyond doubt that, notwithstanding the presence of certain express variation and revocation provisions in the Bill, subsection 33(3) of the *Acts Interpretation Act 1901* continues to apply in relation to other instruments under the Bill.

Clause 238 – Provider of social media service, relevant electronic service, designated internet service or app distribution service

Clause 238 is an interpretive provision. The expressions 'social media service', 'relevant electronic service', 'designated internet service' and 'app distribution service' are defined in clause 5, and several provisions of the Bill refer to such services.

Clause 238(1) provides that, for the purposes of the Bill, a person does not provide a social media service, relevant electronic service or designated internet service merely because the person supplies a carriage service that enables material to be accessed or delivered.

Subclause 238(2) provides that, for the purposes of the Bill, a person does not provide an app distribution service merely because the person supplies a carriage service that enables apps to be downloaded.

A carriage service is defined in the Bill to have the same meaning as in the *Telecommunications Act 1997*, which is 'a service for carrying communications by means of guided and/or unguided electromagnetic energy.'

Subclause 238(3) provides that a person does not provide a social media service, relevant electronic service, designated internet service or app distribution service merely because the person provides a billing service, or a fee collection service, in relation to that service.

Clause 239 – Extended meaning of use

Clause 239 is an interpretative provision. It provides that, unless the contrary intention appears, a reference in the Bill to the 'use' of a thing is a reference to the use of the thing either in isolation or in conjunction with one or more other things. Clause 239 is intended to overcome potential difficulties in attributing instrumentality to a single element of a system, where the whole system is required to perform an act.

Clause 239A – Review of operation of this Act

Clause 239A requires that within 3 years after the commencement of this clause, the Minister must cause to be conducted an independent review of the operation of this Act and legislative rules (clause 240) and whether any amendments to the Act or the rules are required.

Subclause 239A(2) requires the Minister to cause to be prepared a report of this review and subclause 239A(3) requires that, after completion of the report, copies of the report are to be tabled in each House of the Parliament within 15 sitting days of that House.

Clause 240 – Legislative rules

Subclause 240(1) is a standard provision which permits the Minister to make legislative rules for the purposes of the Bill, subject to the exclusions set out in subclause 240(2).