Australian Government

Department of Infrastructure, Transport,
Regional Development and Communications

Online Safety Reform
Regulation Impact Statement

August 2020

Contents

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reforms would also update some elements of the legislation underpinning Australia's online safety regime which are out of date and not flexible enough to deal with emerging issues, such as the rise in the number of social media services and the emergence of new media delivery options. In 2018, an independent review of the *Enhancing Online Safety Act 2015* and Schedules 5 and 7 to the *Broadcasting Services Act 1992* 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 cyberbullying scheme to capture harms occurring on services other than social media;

[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

- 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.

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]

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

[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

[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

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, 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 cyberbullying, 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

[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

[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

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 cyberbullying, and the number of complaints made about serious cyberbullying of Australian children is increasing year on year. In the reporting period 2018-19, the eSafety Commissioner received 531 complaints about cyberbullying.[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 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]

[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 at: https://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

[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

Modest reforms to the already successful cyberbullying 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 cyberbullying 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]
- 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

[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/

[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

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]

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

[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.

statutory investigations into potentially prohibited online content over the previous financial year under Schedules 5 and 7 of the *Broadcasting Services Act 1992* (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 cyberbullying may have lasting effects on young people, including contributing to poor self-esteem and negative mental health outcomes, depression, anxiety and suicidal ideation.[31] A review of studies of cyberbullying, self-harm and suicidal behaviour amongst children and young people published between 1996 and 2017 found that having been a victim or perpetrator of cyberbullying was associated with higher rates of self-harm than for non-victims or non-perpetrators.[32]

[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.

[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.

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 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

[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

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 cyberbullying 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 *Enhancing Online Safety Act 2015* (EOSA), Schedules 5 and 7 to *the Broadcasting Services Act 1992* (BSA) and the *Criminal Code Amendment (Sharing Abhorrent Violent Material) Act 2019.*

[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

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

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 cyberbullying scheme addressing serious cyberbullying 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. Internet service providers 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

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

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.

Internet service providers, 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 cyberbullying and address specific cyberbullying incidents since July 2015, acting as a safety net for victims where cyberbullying material is not removed by social media platforms;
- achieving a 100 per cent success rate in seeking the removal of cyberbullying 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 cyberbullying 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 cyberbullying 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-thirds of Australians played

[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

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.

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 cyberbullying 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 cyberbullying;[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;

[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

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

[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

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

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]

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 cyberbullying 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;

[67] "Submission to the Department of Communications and the Arts", p.11.

[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

- 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
- 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.

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 *Enhancing Online Safety Act 2015* and Schedules 5 and 7 of the *Broadcasting Services Act 1992* into a new online safety Act, including the image-based abuse scheme, cyberbullying 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, cyberbullying 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.

Cyberbullying scheme

The range of services captured under the existing cyberbullying 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 (i.e. Instagram), streaming and video apps (i.e. TikTok) and online gaming services (i.e. 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 X18+ and MA15+ 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 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.

[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

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 cyberbullying 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 cyberbullying 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.

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 cyberbullying 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 cyberbullying 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 cyberbullying, 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.

Cyberbullying and image-based abuse schemes

Recognising that cyberbullying does not occur exclusively on major social media platforms, expanding the scope of the cyberbullying scheme to other services would provide victims of serious cyberbullying 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 cyberbullying 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 cyberbullying complaints

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

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 cyberbullying 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 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.

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

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, 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

[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

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
Cyberbullying scheme	580	0	0	580
Online content scheme	336	0	0	336
Industry codes – Provision of an opt-in filtered internet service	3,638	0	0	3,638
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 notice scheme	21	0	0	21
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.

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 takedown 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.

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 ensure that age verification is 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.

[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

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 Hon Paul Fletcher MP, then 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; 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]

Cyberbullying scheme

Views were received by 28 submissions on a proposal to expand the cyberbullying 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 cyberbullying 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 cyberbullying scheme should occur alongside continued preventative measures by the eSafety Commissioner, including education functions.

[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

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 cyberbullying 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]

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 takedown 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*.

[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

[86] Bose, "Consultation on a new Online Safety Act – Submission", p.12.

[87] "Submission to the Department of Communications and the Arts", p.9.

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 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.

[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.

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, internet service providers, 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.

Cyberbullying 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[i]	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[ii]	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[iii]	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**	
Cyberbullying 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 cyberbullying 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 cyberbullying 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 cyberbullying 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**	

[i] A small business is a business accessible to Australians with less than 20 employed persons.

[ii] A medium business is a business accessible to Australians with between 20 to 199 employed persons.

[iii] A large business is a business accessible to Australians with more than 200 employed persons.