Australian Government

Australian Government response to the Senate Legal and Constitutional Affairs References Committee report:

Adequacy of existing offences in the Commonwealth Criminal Code and of state and territory criminal laws to capture cyberbullying

April 2021

[This page is left intentionally blank.]

Contents

Background

On 7 September 2017, the Senate referred the following matter to the Committee for inquiry and report by 29 November 2017:

> The adequacy of existing offences in the Commonwealth Criminal Code and of state and territory criminal laws to capture cyberbullying, including:
>
> a. the broadcasting of assaults and other crimes via social media platforms;
> b. the application of section 474.17 of the Commonwealth Criminal Code 'Using a carriage service to menace, harass or cause offence', and the adequacy of the penalty, particularly where the victim of cyberbullying has self-harmed or taken their own life;
> c. the adequacy of the policies, procedures and practices of social media platforms in preventing and addressing cyberbullying;
> d. other measures used to combat cyberbullying predominantly between school children and young people; and
> e. any other related matter.

On 19 October 2017 the Senate extended the Committee's reporting date to the last sitting day in March 2018.

Over the course of the inquiry, the Committee received 34 submissions, of which three were received *in camera.* The Committee held two public hearings. The first hearing was in Canberra on 9 February 2018 and the second in Melbourne on 7 March 2018.

The Committee's final report was tabled and released on 28 March 2018. The Committee made nine recommendations.

Response methodology

The Department Infrastructure, Transport, Regional Development and Communications has coordinated the development of the Australian Government's response, with input from Commonwealth agencies including the Office of the eSafety Commissioner (eSafety), the Attorney-General's Department, the Department of Home Affairs, the Australian Federal Police (AFP), the Department of Education, the Department of Health, the Department of Social Services and, in relation to Recommendation 4, state and territory governments through the Department of Home Affairs.

Summary of Australian Government's Response to Recommendations

Recommendation	Response
Recommendation 1 The committee recommends that the Australian Government consult state and territory governments, non-government organisations, and other relevant stakeholders, to develop and publicise a clear definition of cyberbullying that recognises the breadth and complexity of the issue.	**Supported**
Recommendation 2 The committee recommends that Australian governments approach cyberbullying primarily as a social and public health issue. With this in mind, the committee recommends that Australian governments consider how they can further improve the quality and reach of preventative and early intervention measures, including education initiatives, both by government and non-government organisations, to reduce the incidence of cyberbullying among children and adults.	**Supported in principle**
Recommendation 3 The committee recommends that the Senate not legislate to increase penalties for cyberbullying offences committed by minors beyond the provisions already in place.	**Supported**
Recommendation 4 Noting the serious harms that cyberbullying can cause, the committee recommends that Australian governments ensure that: • the general public has a clear awareness and understanding of how existing criminal offences can be applied to cyberbullying behaviours; • law enforcement authorities appropriately investigate and prosecute serious cyberbullying complaints under either state or Commonwealth legislation, coordinate their investigations across jurisdictions where appropriate, and make the process clear for victims of cyberbullying, and • consistency exists between state, territory and federal laws in relation to cyberbullying.	**Supported in principle**
Recommendation 5 The committee recommends that the Australian Government consider increasing the maximum penalty for using a carriage service to menace, harass, or cause offence under section 474.17 of the *Criminal Code Act 1995* from three years' imprisonment to five years' imprisonment.	**Supported**

Recommendation	Response
Recommendation 6 The committee recommends that the Australian Government: • ensure that the Office of the eSafety Commissioner is adequately resourced to fulfil all its functions, taking into account the volume of complaints it considers; • promote to the public the role of the Office of the eSafety Commissioner, including the cyberbullying complaints scheme; • consider the improvements to the process by which the Office of the eSafety Commissioner can access relevant data from social media services hosted overseas, including account data, that would assist the eSafety Office to apply the end-user notice scheme; • consider whether amendments to the *Enhancing Online Safety Act 2015* relating to the eSafety Commissioner and the cyberbullying complaints scheme would be beneficial, and in particular, o expanding the cyberbullying complaints scheme to include complaints by adults; o expanding the application of the tier scheme by amending the definitions of 'social media service' and 'relevant electronic service', and o increasing the basic online safety requirements for social media services.	**Supported in principle**
Recommendation 7 The committee recommends that the Australian Government place and maintain regulatory pressure on social media platforms to both prevent and quickly respond to cyberbullying material on their platforms, including through the use of significant financial penalties where insufficient progress is achieved.	**Supported in principle**
Recommendation 8 The committee recommends that the Australian Government legislate to create a duty of care on social media platforms to ensure the safety of their users.	**Noted**
Recommendation 9 The committee recommends that the Australian Government consider requiring social media platforms to publish relevant data, including data on user complaints and the platforms' responses, as specified by the eSafety Commissioner and in a format specified by the eSafety Commissioner.	**Supported in principle**

Cyberbullying is a complex social issue

The Committee's report notes that cyberbullying is a complex social issue which requires a multifaceted response and cannot be addressed by criminal sanctions alone. The Australian Government is taking a comprehensive approach to cyberbullying by pursuing a range of measures. As noted in the report, Commonwealth criminal offences already capture the most serious cases of cyberbullying. The Government considers that education, victim support, and civil avenues are just as important as recourse to criminal law to effectively address cyberbullying.

Early intervention measures such as education, harm minimisation and encouraging the safe and responsible use of technology are proactive measures that can prevent cyberbullying conduct escalating to criminal behaviour and prevent or minimise the harm resulting from cyberbullying incidents.

The Government considers such education and awareness building measures to be important initiatives to combat the causes of cyberbullying behaviour than criminal offences. The Government notes that similar sentiments were expressed in Queensland's Anti-Cyberbullying Taskforce report, *Adjust our settings: a community approach to address cyberbullying among children and young people in Queensland*, and in the Queensland Government's response to that report.[1]

A number of meaningful initiatives aimed at understanding and addressing the complex factors which contribute to cyberbullying are already underway. For example, on 9 February 2018 the Council of Australian Governments (COAG) agreed to establish a senior officials' working group on bullying and cyberbullying, led by the COAG Education Council.

The Minister for Education is leading this work on behalf of the Commonwealth. The group delivered its *Enhancing community responses to student bullying, including cyberbullying* report and work program to the COAG Education Council on 14 September 2018.[2] The report and work program were considered by COAG in December 2018.

The Government acknowledges that cyberbullying is a modern and evolving social concern within the community, and is a particular concern for students, teachers and parents. Further, access to the online world is a basic requirement for community and employment participation, and as such, it should not be an ungoverned space. The targets of online abuse and bullying should not be forced offline. Instead, technology platforms, governments and other users must all play a part in making the internet safe.

[1] Queensland Department of the Premier and Cabinet, 15 October 2018, Government response to the Queensland Anti-Cyberbullying Taskforce report, available at campaigns.premiers.qld.gov.au/antibullying/taskforce/

[2] COAG Education Council, *Communique*, 14 September 2018, available at www.educationcouncil.edu.au/EC-Communiques-and-Media-Releases.aspx

Australian Government response to Recommendations

Recommendation 1

5.4 The committee recommends that the Australian Government consult state and territory governments, non-government organisations, and other relevant stakeholders, to develop and publicise a clear definition of cyberbullying that recognises the breadth and complexity of the issue.

The Australian Government **supports** Recommendation 1, and recognises the importance of having a nationally consistent understanding of what behaviour constitutes cyberbullying, in order to support the development of appropriate and effective policy responses. Consultation with states and territories on this important social issue is vital. Developing a better understanding of cyberbullying was recognised as a priority by the Council of Australian Governments (COAG) at its February 2018 meeting[3], and was considered throughout 2018 by the COAG Education Council. COAG is the appropriate forum to ensure the involvement of states and territories, and to facilitate engagement with relevant non-government stakeholders.

The work of the COAG Education Council is outlined below.

COAG Senior officials' working group

Through the COAG Education Council, a Bullying and Cyberbullying Senior Officials Working Group was established. The strategic objectives of the Working Group were to:

- consider the underlying drivers of bullying and cyberbullying;
- develop an agreed national definition of bullying and cyberbullying to establish a common language for school communities;
- share strategies and best practice approaches to address bullying and cyberbullying and consider the available evidence on what makes these approaches effective; and
- establish a work program for the Education Council based on these objectives.

The Working Group operated from May 2018 and developed a work program which was endorsed by the COAG Education Council in September 2018.[4] The work program was noted by COAG in December 2018.[5] COAG has sinced ceased to exist with its final meeting taking place in March 2020.

The Working Group was chaired by the Commonwealth Department of Education and Training. Other Commonwealth representatives included the Department of the Prime Minister and Cabinet and the then Department of Communications and the Arts. eSafety contributed as a national agency. The Department of Home Affairs and the Attorney-General's Department were key consultative partners. Two nominated members from each of the states and territories represented the views of First Ministers, Health, Justice and Education departments.

Working Group endorsed national definition on bullying and cyberbullying

The Bullying and Cyberbullying Senior Officials Working Group developed a national definition on bullying and cyberbullying to be used in school communities and promoted to and by relevant

[3] COAG, *Communique*, 9 February 2018, www.coag.gov.au/meeting-outcomes/coag-meeting-communiqu%C3%A9-9-february-2018. The eSafety Commissioner, Ms Julie Inman Grant, presented to the COAG Education Council about the eSafety's cyberbullying work at the Council's meeting held on 22 June 2018, www.educationcouncil.edu.au/site/DefaultSite/filesystem/documents/EC%20Communiques%20and%20media%20releases/Education%20Council%20Communique%2022%20June%202018%20-%20final.pdf.

[4] *Enhancing community responses to student bullying, including cyberbullying: Report and Work Program,* as endorsed at the Twentieth Education Council Meeting, 14 September 2018, www.coag.gov.au/sites/default/files/communique/bcsowg-report-work-program.pdf

[5] COAG, *Communique*, 12 December 2018, www.coag.gov.au/meeting-outcomes/coag-meeting-communique-12-december-2018.

stakeholders. The definition is intended for policy frameworks and is not intended to be used as a legal definition. The definition has been reviewed by three anti-bullying experts.

> *Bullying is an ongoing and deliberate misuse of power in relationships through repeated verbal, physical and/or social behaviour that intends to cause physical, social and/or psychological harm. It can involve an individual or a group misusing their power, or perceived power, over one or more persons who feel unable to stop it from happening.*
>
> *Bullying can happen in person or online, via various digital platforms and devices and it can be obvious (overt) or hidden (covert). Bullying behaviour is repeated, or has the potential to be repeated, over time (for example, through sharing digital records).*
>
> *Bullying of any form or for any reason can have immediate, medium and long-term effects on those involved, including bystanders.*
>
> *Single incidents and conflict or fights between equals, whether in person or online, are not defined as bullying.*

The Working Group recommended this definition is used by all schools and promoted to relevant stakeholders.

Recommendation 2

5.7 The committee recommends that Australian governments approach cyberbullying primarily as a social and public health issue. With this in mind, the committee recommends that Australian governments consider how they can further improve the quality and reach of preventative and early intervention measures, including education initiatives, both by government and non-government organisations, to reduce the incidence of cyberbullying among children and adults.

The Australian Government **supports in principle** Recommendation 2**.** In addition to the work undertaken by the COAG Education Council outlined in the response to Recommendation 1, the Government committed an additional $17 million to online safety as part of the Keeping our Children Safe Online package in the Mid-Year Economic and Fiscal Outlook 2018-19 (MYEFO 2018-19).

This package is in addition to the ongoing work of eSafety which has an established education and prevention program for schools. This work includes virtual classrooms (providing online safety education directly to students); teacher professional learning (to equip teachers with the knowledge and skills to teach online safety in the classroom); training for Chaplains; guidance and resources to support parents; an accreditation program for non-government organisations to deliver online safety education programs and Best Practice Guidance for schools to support them to prevent and respond to online harms, including cyberbullying.

Keeping Our Children Safe Online package and other Australian Government online safety initiatives

The Keeping our Children Safe Online package provided funding for the National Online Safety Awareness Campaign*, Start the Chat,* which aimed to raise awareness of the resources available to parents to protect their children online, and for eSafety to develop and deliver an early years online safety program. The package also establishes an online safety research program. The research program will enable a better understanding of online safety risks, including cyberbullying, and ensure that measures developed have a solid evidence base. The early years online safety program recognises that online safety is important for even very young children. This initiative will make additional and age-specific resources available to parents and carers to inform them on how to provide a safe online environment for young children. It will also establish and roll out a competency-based online safety training module for early childhood workers to give them the necessary tools and information to promote and teach safe online behaviours.

The Government notes that these measures will complement meaningful work that is already being undertaken by numerous government and non-government organisations (NGOs). In recognition of the important work undertaken by NGOs, the Government established a $10 million NGO grants program to be administered by eSafety over the next four years.[6] The first grant recipients of the Australian Government's Online Safety Grants Program were announced in October 2020. The grants program supports NGOs with expertise in online safety to deliver high value online safety education and training projects.

Cyberbullying amongst adults

The Government recognises that online cyberbullying can affect both adults and children, however adults have greater access to avenues to seek redress. There are criminal laws, which apply to using the internet to menace and harass people of all ages. In the civil context, an array of actions and various forms of liability may apply, including defamation, breach of confidence, invasion of privacy or trespass to person.[7]

[6] Department of Communications and the Arts, 3 April 2019, *Budget 2019-20*, available at https://www.communications.gov.au/departmental-news/budget-2019-20

[7] See, for example, *Giller v Procopets*; [2008] VSCA 236; *Wilson v Ferguson* [2015] WASC 15.

The Government also proposed to establish a cyber abuse scheme for adult victims under the new Online Safety Act. This new scheme would introduce civil penalties for cyber abuse against adult victims, and empower the eSafety Commissioner to issue 24-hour takedown notices. A discussion paper detailing the proposal was released on 11 December 2019 for public consultation.[8] This led to the development of a draft of an Online Safety Bill which was released for consultation on 23 December 2020.[9] The Government introduced the Bill for a new Online Safety Act into Parliament on 24 February 2021 and referred to Committee, with a hearing held on 5 March.

The Government will continue working with stakeholders to develop the cyber abuse scheme. This work has also been informed by the findings of an independent review of online safety legislation by Lynelle Briggs AO. Further information about the independent review is outlined under Recommendation 6.

Device use in schools

The Australian Government is concerned about the impact of mobile phones and other digital devices on student wellbeing and learning outcomes. For example, youth mental health provider 'headspace' reports that over 50 per cent of 12 to 25 year olds have been cyberbullied at some time. While students need to become digitally literate and gain knowledge and skills to be safe and responsible users of digital technology, the Government believes that regulating the use of mobile phones in the classroom will encourage students to focus on learning by removing a significant distraction.

The Government has delivered on its election commitment to work with state and territory governments to develop best practice policies on mobile phone use in classrooms. In 2019 the Government engaged an independent researcher to review existing evidence about the impact of mobile phone use on learning outcomes and student wellbeing, including cyberbullying. The findings were presented to Education Council at its meeting in September 2019. Education Council also heard from other international experts about the impact of technology on young people, and best practice policies for managing potential issues such as cyberbullying.

A number of states have since announced restrictions on the use of mobile phones in government schools from 2020 onwards, including New South Wales, Victoria, Tasmania and Western Australia.

While the Government takes a national leadership role in education, decisions about how technology is used in schools are a matter for state and territory governments and individual schools. The Government supports any state or territory government that restricts mobile phones in schools and will work with jurisdictions to limit the inappropriate use of such devices.

[8] Department of Communications and the Arts, December 2019, *Online Safety Legislative Reform: Discussion Paper,* available at: https://www.communications.gov.au/have-your-say/consultation-new-online-safety-act

[9] Department of Infrastructure, Transport, Regional Development and Communications, December 2020 https://www.communications.gov.au/have-your-say/consultation-bill-new-online-safety-act

Recommendation 3

5.12 The committee recommends that the Senate not legislate to increase penalties for cyberbullying offences committed by minors beyond the provisions already in place.

The Australian Government **supports** this recommendation, noting the existing Commonwealth offences that can apply to cyberbullying behaviour apply to the conduct of adults and minors. However, increasing penalties for existing offences covering cyberbullying risks disproportionately impacting children and young people as they may often be both perpetrators and victims of cyberbullying. It is long-standing Government policy to avoid over-criminalising the conduct of minors, unless that conduct is malicious or exploitative, with criminal sanctions being considered an option of last resort.

To address cyberbullying between minors, it is important to focus on education and community engagement measures which address the underlying causes of serious cyberbullying, rather than on punitive measures, such as increasing criminal penalties.

Penalties for existing Commonwealth offences

As noted in the Committee's report, young people are often the first to take up new and emerging technologies and social media platforms, making them more likely to be both the perpetrators and victims of cyberbullying. Therefore, increasing penalties for cyberbullying offences could lead to unintended and disproportionate criminalisation of the conduct of minors.

The Government notes this recommendation may also be relevant to states and territories in respect of relevant offences and penalties.

Applying prosecutorial discretion to prosecutions against minors

The Government supports retaining the existing offences and penalties, which provide a range of prosecutorial options, depending on the seriousness of the behaviour. The Government also notes the importance of prosecutorial discretion, to avoid over-criminalising the conduct of minors. Commonwealth, state and territory prosecutorial agencies hold the ultimate discretion to pursue a prosecution once it has been referred by the investigating law enforcement agency. Prosecutors must consider whether instituting or continuing prosecution is in the public interest, among other considerations.

Recommendation 4

5.13 Noting the serious harms that cyberbullying can cause, the committee recommends that Australian governments ensure that:

- the general public has a clear awareness and understanding of how existing criminal offences can be applied to cyberbullying behaviours;
- law enforcement authorities appropriately investigate and prosecute serious cyberbullying complaints under either state or Commonwealth legislation, coordinate their investigations across jurisdictions where appropriate, and make the process clear for victims of cyberbullying, and
- consistency exists between state, territory and federal laws in relation to cyberbullying.

The Australian Government **supports** this recommendation **in principle** and will continue working with state and territory governments to promote a harmonised response to cyberbullying.

Education resources

The Government is committed to enhancing awareness of the existing Commonwealth offences that apply to criminal cyberbullying conduct. Education for the public and for law enforcement is vital to the appropriate application of existing offences to criminal cyberbullying.

The AFP's existing ThinkUKnow program provides cyber safety presentations to parents, carers and teachers, and school-aged children between five and 18. Programs for older students include discussion of the criminal aspects of online behaviours. There are a variety of additional education programs offered by eSafety, state and territory agencies, and non-government organisations.

The AFP, through ThinkUKnow program training, will continue to work with eSafety to provide advice to state and territory police on the role of eSafety, including the process for making a serious cyberbullying complaint.

The AFP will support the work of eSafety in providing education resources to law enforcement and the public.

Further actions

The AFP and eSafety , in consultation with the Department of Home Affairs, will update websites so that available criminal offences are clearly advised to the general public on the ThinkUKnow and eSafety websites, to provide guidance on applicable criminal offences.

Through the ThinkUKnow program, the AFP will continue to engage with state and territory police to build greater awareness of Commonwealth offences that apply to cyberbullying behaviours as well as promoting the role of eSafety in addressing serious cyberbullying material.

National principles and approach

In addition to the Commonwealth *Criminal Code 1995* (the Criminal Code), states and territories have various state-based offences available to them to prosecute cyberbullying behaviours and undertake a range of measures to combat cyberbullying.

The Australian Government will work with states and territories through existing forums to explore developing national principles to support a nationally consistent approach to combatting criminal cyberbullying. This includes the development of a coordinated, national approach to criminal cyberbullying and online harassment through the Council of Attorneys-General. Noting that a number of states and territories have existing offences relating to criminal cyberbullying, the principles would constitute non-binding guidance to assist jurisdictions when developing or reviewing criminal offences targeting cyberbullying, and developing investigative processes and procedures for coordination across jurisdictions.

Recommendation 5

5.15 The committee recommends that the Australian Government consider increasing the maximum penalty for using a carriage service to menace, harass, or cause offence under section 474.17 of the *Criminal Code Act 1995* from three years' imprisonment to five years' imprisonment.

The Australian Government **supports** this recommendation.

Criminal offences for cyberbullying only address behaviour once the harm to victims has already occurred. In general, it is preferable to adopt early intervention measures such as education, harm minimisation and encouraging the safe and responsible use of technology, which can prevent or reduce the number of cyberbullying incidences. However, available penalties should also send a clear message to perpetrators of abuse and harassment that this behaviour will not be tolerated.

Criminal penalties

Criminal offences, and accordingly the Commonwealth Criminal Code, should remain consistent with community expectations and responsive to developments in anti-social behaviour. The maximum penalty applied to an offence should be sufficient to punish a worst case offence, provide an effective deterrent to the commission of the offence, and reflect the seriousness of the offence within the relevant legislative scheme. The Government acknowledges that the rapid growth in online connectivity and the use of social media may see a corresponding increase in the volume and/or gravity of offending under section 474.17 of the Criminal Code. As such, the Government has committed to increasing the maximum penalty for those using a carriage service to menace, harass or cause offence from three years' imprisonment to five years' imprisonment in order to send a deterrence signal and to meet community expectations.

The Government **notes** Recommendation 3, which recommends not legislating to increase penalties for cyberbullying offences committed by minors. Cyberbullying, sexting, and other anti-social online behaviours are increasingly engaged in by children and young people. As a result there is a risk that any new offences or penalties for cyberbullying will disproportionately apply to children, while not necessarily addressing the underlying causes of cyberbullying, or preventing the harm that it causes to victims. Criminal sanctions for minors in particular should generally be an option of last resort.

The Government notes the broad application of section 474.17 of the Criminal Code, which captures a range of different behaviours that are not related to cyberbullying, including stalking, domestic violence, and other threatening or intimidating communications conducted using a carriage service. As the definition of 'carriage service' is not limited to the internet, section 474.17 applies also to telephone communications. As such, increasing the available penalties under this offence may also impact the penalties available (and likely to be imposed by a court) for the other types of behaviour (such as menacing or harassing telephone calls) captured by this offence.

Current Commonwealth Criminal Code offences and penalties

The Criminal Code contains broad offences that cover cyberbullying, within the limits of Commonwealth power. A number of Commonwealth offences address cyberbullying behaviours. As noted in a number of submissions to the inquiry, only the most serious cases of cyberbullying warrant criminal sanctions.

Section 474.17 of the Criminal Code sets out the offence of using a carriage service to menace, harass or cause offence. Section 474.17 has been successfully applied to the prosecution of cyberbullying, including behaviour such as:

- posting offensive and abusive comments on Facebook tribute pages of deceased children;
- sending taunting and abusive messages on social media, and posting photos on Instagram with offensive commentary concerning a victim; and
- in the context of underage grooming, posting inappropriate commentary and manipulative and threatening comments on Facebook accounts of underage girls.[10]

[10] R v Hampson [2011] QCA 13, Grott v The Commissioner of Police [2015] QDC 142, Aboud v R [2017] NSWCCA 140, and Agostino v Cleaves [2010] ACTSC 19.

The *Enhancing Online Safety (Non-consensual Sharing of Intimate Images) Act 2018* introduced specific criminal offences into the Criminal Code for use of a carriage service to transmit private sexual material. There have been instances of cyberbullying that have involved image based abuse. The new aggravated criminal offences at section 474.17A provide maximum penalties of up to five years' imprisonment for using a carriage service menace, harass or cause offence involving the transmission of private sexual material, and up to seven years' imprisonment where the perpetrator has previously had three or more civil penalty orders made against them for the non-consensual sharing of intimate images. The new aggravated offences came into effect on 1 September 2018.

Section 474.14 of the Criminal Code contains an offence for using a carriage service to commit a serious offence. This captures using the internet or a phone to commit or attempt to commit any Commonwealth, state or territory offence with a maximum penalty of five years' imprisonment or more. In the cyberbullying context, this offence can be used to connect the online nature of conduct with traditional offences for stalking, harassment and threats.

Further, section 474.15 of the Criminal Code contains an offence for using a carriage service to make a threat to kill or cause serious harm, which can apply to threats made in the context of cyberbullying. This offence carries a maximum penalty of 10 years' imprisonment for a threat to kill, and seven years' imprisonment for a threat to cause serious harm.

The prescribed maximum penalties for these Commonwealth offences are designed to deter and punish the worst case offences, including repeat offences. Courts are required to consider the harm suffered by the victim as a result of the offence during sentencing, including the personal circumstances of any victim of the offence. Therefore, where the harm to the victim is significant (for example, if the victim has attempted to take their own life as a result of the cyberbullying they endured) this will be a factor which the court considers when determining the appropriate penalty.

Proposed increase in criminal penalties

The Government introduced the Online Safety Bill into Parliament on 24 February 2021. In concert with the Bill, the Government proposes to increase the maximum penalty for:

- section 474.17(1) (menace, harass or cause offence) from 3 years to 5 years imprisonment
- section 474.17A(1) (menace, harass or cause offence involving private sexual material) from 5 years to 6 years imprisonment.

Recommendation 6

5.22 The committee recommends that the Australian Government:

- ensure that the Office of the eSafety Commissioner is adequately resourced to fulfil all its functions, taking into account the volume of complaints it considers;
- promote to the public the role of the Office of the eSafety Commissioner, including the cyberbullying complaints scheme;
- consider improvements to the process by which the Office of the eSafety Commissioner can access relevant data from social media services hosted overseas, including account data, that would assist the eSafety Office to apply the end-user notice scheme;
- consider whether amendments to the *Enhancing Online Safety Act 2015* relating to the eSafety Commissioner and the cyberbullying complaints scheme would be beneficial, and in particular, consider:
  - expanding the cyberbullying complaints scheme to include complaints by adults;
  - expanding the application of the tier scheme by amending the definitions of 'social media service' and 'relevant electronic service', and
  - increasing the basic online safety requirements for social media services.

The Australian Government **supports** this recommendation **in principle**.

Resourcing and promoting the role of the eSafety Commissioner

The Government has ensured that eSafety is adequately resourced.

As part of the 2018/19 Budget, the Government committed an additional $14.2 million over four years for eSafety to provide online safety advice and support to all Australians. This funding included:

- $1.2 million for the eSafety Women program. The additional funding will enable eSafety to continue providing advice to front line workers to help women experiencing online abuse, particularly in domestic violence cases.
- $1.2 million for the certified providers program (renamed as the Trusted eSafety Provider Program). Under this program, eSafety certifies trainers to provide online safety education, including about cyberbullying, in schools, and runs workshops designed to equip trainee teachers at university with online safety skills to support their future students.
- $1.7 million for the development of cyber abuse materials, including targeted resources for vulnerable Australians experiencing online abuse, including:
  - pre-school aged children;
  - children and adults in the Lesbian, Gay, Bisexual, Transgender, Queer and Intersex (LGBTQI) community;
  - people from culturally and linguistically diverse backgrounds;
  - Indigenous Australians; and
  - Australians with disability.
- $4.0 million for the civil penalty regime for the non-consensual sharing of intimate images.
- $6.0 million to strengthen the eSafety's IT infrastructure.

In December 2018, the Government announced the $17 million 'Keeping Our Children Safe Online' package which committed additional resources to support parents, teachers and carers of children aged under 5 years, as well as funding a new annual national eSafety survey, a new national awareness campaign, and the development of an online safety charter.

In February 2019, the Government announced $10 million to enable NGOs to deliver practical online safety education and training projects. Also in February 2019, the Government announced that eSafety will also receive over $1 million in funding through the Women's Safety Package Technology Trials program for three projects, including one to study the ways children unintentionally disclose their identifying information to perpetrators of technology-facilitated abuse, and how to reduce this risk.

In March 2019, the Government committed a further $4 million to online safety through programs to be delivered by eSafety as part of the Fourth Action Plan of the *National Plan to Reduce Violence against Women and their Children 2010-2022*.

In June 2020, the Government announced a $10 million funding boost to assist the eSafety Commissioner to respond to an increase in demand for support during COVID-19.

As part of the 2020-21 Budget, the Government committed to providing $39.4 million over 3 years in new funding to the eSafety Commissioner. This will allow the eSafety Commissioner to:

- respond to a sustained increase in demand for its programs and resources,
- provide Australians with strong and effective support to stay safe as they work, learn and engage online, and
- fulfil additional functions under the proposed new Online Safety Act.

Data access by eSafety

The Committee has highlighted the difficulties faced by eSafety in accessing relevant data to apply its end-user notice scheme, particularly where telecommunications service providers hold information on servers located outside of Australia. The challenges associated with accessing data located overseas are also faced more broadly by law enforcement in investigating and addressing technology-facilitated crime.

Currently, law enforcement are able to make requests to foreign countries for assistance under the *Mutual Assistance in Criminal Matters Act 1987* (MACMA). However, as the cyberbullying end-user notice scheme is a civil regime, eSafety is unable to make requests under the MACMA. The Government notes there are already specific measures under the *Telecommunications Act 1997* that permit the disclosure of certain information to the eSafety Commissioner for the purposes of carrying out the Commissioner's functions. Also, if a cyberbullying matter has reached the threshold of criminality, eSafety can refer it to state and territory police under section 80 of the *Enhancing Online Safety Act 2015* (Cth) for investigation and potential prosecution. The Government supports improving the process for identifying and referring matters to the state and territory police which reach this criminal threshold.

The Government supports improvements to the process by which eSafety can access relevant data within existing frameworks to discharge its functions, noting that the end-user notice scheme is a civil regime and eSafety is not a criminal law enforcement agency. The Government supports developing relationships and improving processes between eSafety and platform providers to achieve better outcomes with requests for voluntary non-content data.

Independent review of the *Enhancing Online Safety Act 2015*

The *Enhancing Online Safety Act 2015* requires that a statutory review of the Act be conducted within three years of the commencement of the Act. The review commenced in June 2018 and the report of the review was tabled in Parliament on 15 February 2019.

The former Minister for Communications and the Arts appointed Ms Lynelle Briggs AO as the independent reviewer to undertake this statutory review. Ms Briggs concurrently reviewed the operation of Schedules 5 and 7 of the *Broadcasting Services Act 1992*, which establishes the removal scheme for prohibited and potentially prohibited content including child sexual abuse material, to ensure a comprehensive consideration of all legislation administered by eSafety.

The review considered:

- the operation of the *Enhancing Online Safety Act 2015* and its provisions, including the cyberbullying scheme;
- the eSafety's remit and whether the current functions and powers in the Act are sufficient to allow the Commissioner to perform those functions effectively; and
- whether the current governance structure and support arrangements for the Commissioner are fit for purpose.

The Briggs Review found that the world-leading initiative of the Office of the eSafety Commissioner has achieved much success since it was established in 2015. The independent review has made five recommendations, including a key proposal for a single consolidated piece of online safety legislation, and including greater transparency and reporting requirements for industry.

The Government is committed to ensuring the best online safety arrangements and maintaining Australia as a world-leader on this issue. This will involve continuing to work with technology firms to improve online safety to have devices and services marketed to children default to the most restricted safety and privacy settings, making available the option of a filtered internet service, and ensuring information about safety and parental control settings are available at all points in the supply chain.

A new Online Safety Act

The Government has committed to introducing a new Online Safety Act to consolidate and update regulatory arrangements in light of changes to the digital environment.

On 11 December 2019, the Government released the online safety legislation reform discussion paper which outlined the key elements of a proposed new Online Safety Act.[11] The proposed elements of a new Act include:

- A set of basic online safety expectations for industry that make clear the community's expectations for online safety, with associated reporting requirements.
- An enhanced cyberbullying scheme for Australian children to capture the range of online services that they are using, and not just social media platforms.
- A new cyber abuse scheme for Australian adults to facilitate the removal of serious online abuse and harassment, supported with a civil penalty regime.
- Consistent take-down requirements for image-based abuse, cyber abuse, cyberbullying and seriously harmful online content, requiring online service providers to remove such material within 24 hours of being requested to do so by the eSafety Commissioner.
- A reformed online content scheme that would require the Australian technology industry to be proactive in addressing access to harmful online content and that would expand the eSafety Commissioner's powers to address illegal and harmful content hosted overseas.
- An ancillary service provider scheme to empower the eSafety Commissioner to disrupt access to seriously harmful online material made available via search engines, app stores and other ancillary service providers.
- An additional power for the eSafety Commissioner to respond rapidly to an online crisis event (such as the Christchurch terrorist attacks) by requesting internet service providers block access to terrorist and extreme violent content.
- After considering the feedback received in response to this consultation, the Government developed an Online Safety Bill. This was released for consultation on 23 December 2020.[12]On 24 February 2021, the Government introduced the Online Safety Bill into Parliament. The Bill was referred to Committee and a hearing held on 5 March 2021.

[11] Department of Communications and the Arts, December 2019, *Online Safety Legislative Reform: Discussion Paper,* available at: https://www.communications.gov.au/have-your-say/consultation-new-online-safety-act

[12] Department of Infrastructure, Transport, Regional Development and Communications, December 2020 https://www.communications.gov.au/have-your-say/consultation-bill-new-online-safety-act

Recommendation 7

5.27 The committee recommends that the Australian Government place and maintain regulatory pressure on social media platforms to both prevent and quickly respond to cyberbullying material on their platforms, including through the use of significant financial penalties where insufficient progress is achieved.

The Australian Government **supports** this recommendation **in principle.**

The Government notes that there are effective regulatory measures in place to require social media platforms to remove cyberbullying material directed at Australian children, including financial penalties of up to $105,000 for corporations for failure to comply with a social media service notice issued by the eSafety Commissioner under section 35 of the *Enhancing Online Safety Act 2015*. eSafety works closely with social media partners and relevant electronic service providers to remove cyberbullying material swiftly – in some cases, less than 30 minutes. The scheme supports a collaborative approach between eSafety and industry.

Safety by Design

Following consultation with industry, key stakeholders, parents and carers eSafety released in July 2019 its Safety by Design Principles.

These principles provide a path to guide the development of safer online environments by industry. They directly place safety and the rights of users at the centre of the design, deployment and development of online products and services.

Online Safety Charter

The Government recognises that digital platforms can do more to be proactive in addressing cyberbullying and other forms of technology-facilitated abuse. On 11 December 2019, the Minister for Communications, Cyber Safety and the Arts, the Hon Paul Fletcher MP, released the Government's Online Safety Charter.

The Online Safety Charter sets out Government's expectations for technology firms and digital platforms to protect Australians from harmful online experiences. It is based on the premise that behaviour that is unacceptable offline should not be tolerated or enabled online, and that content that is harmful to users, particularly children, should be appropriately restricted. Technology firms and digital platforms have a responsibility to respect the rights and dignity of users online and to take meaningful action to address and prevent harms being incurred by those using their products or services.[13]

Online Safety Act

On 24 February 2021, the Government introduced the Bill for a new Online Safety Act into Parliament. The new Act will maintain and enhance measures that are in place to deal with cyberbullying under the *Enhancing Online Safety Act 2015*, and see that they continue to be effective in a contemporary digital media environment. In developing the new Act, consideration has been given to measures to augment and support the Online Safety Charter and enhance the transparency of actions taken by industry to ensure the safety of their users.

[13] *Online Safety Charter,* accessible at: https://www.communications.gov.au/documents/online-safety-charter-0

Recommendation 8

5.28 The committee recommends that the Australian Government legislate to create a duty of care on social media platforms to ensure the safety of their users.

The Australian Government **notes** this recommendation and will closely monitor work being done in other jurisdictions about creating a legislated duty of care for social media platforms and large technology firms.

The Government considers that online safety is a shared responsibility, and that content and behaviour which is prohibited offline should also be prohibited online. The Government considers that social media platforms and other technology firms need to recognise that their responsibility for tackling harmful behaviours and content goes hand-in-hand with their influential and important position within Australian society. It is particularly important that industry participants whose products and services are used by children take appropriate action to uphold the safety of their users.

The Government continues to support and progress measures that pressure industry to lift online safety standards. In July 2019, eSafety released its Safety by Design principles to encourage developers to consider user safety at the centre of design, development and deployment of online products and services. In December 2019, the Government released the Online Safety Charter which sets out expectations for technology firms and digital platforms to protect Australians from harmful online experiences.
The Government has indicated that where technology companies fall short of community standards, it will consider regulatory options to uphold the safety of Australians online. As noted in response to recommendation 6, work is being progressed to consolidate and modernise regulatory arrangements through the development of a new Online Safety Act. The Bill for a new Online Safety Act was introduced into Parliament on 24 February 2021. The Bill was referred to Committee and a hearing was held on 5 March 2021.

Recommendation 9

5.31 The committee recommends that the Australian Government consider requiring social media platforms to publish relevant data, including data on user complaints and the platforms' responses, as specified by the eSafety Commissioner and in a format specified by the eSafety Commissioner.

The Australian Government **supports** this recommendation **in principle**.

The Government recognises that there is a greater need for accountability and transparency by social media services and other digital platforms. Consultation undertaken by eSafety during the development of the Safety by Design Principles demonstrated a real need for an approach to online safety that required transparency and accountability. This is acknowledged by principle 3: Transparency and Accountability.

The Online Safety Charter, discussed in the response to Recommendation 7, includes an expectation for firms operating in the Australian digital media market to publish annual assessments of reported abuses on services, alongside the open publication of meaningful analysis of metrics such as abuse data and reports, the effectiveness of moderation efforts and the extent to which community standards and terms of service are being satisfied through enforcement metrics.

More broadly, the Government has considered the accountability of social media services and other digital platforms for online safety in the Online Safety Bill introduced into Parliament on 24 February 2021. The new Act will establish a modern, fit-for-purpose regulatory framework for tackling online harms in Australia, and this will include appropriate obligations for social media and other services that are being used every day by Australian children and adults.