The Senate

Legal and Constitutional Affairs References Committee

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

March 2018

ISBN 978-1-76010-739-0

This document was produced by the Senate Legal and Constitutional Affairs Committee secretariat and printed by the Senate Printing Unit, Department of the Senate, Parliament House, Canberra.

Members of the committee

Members

Senator Louise Pratt (ALP, WA) (Chair)

Senator the Hon Ian Macdonald (LNP, QLD) (Deputy Chair)

Senator Kimberley Kitching (ALP, VIC)

Senator Nick McKim (AG, TAS)

Senator Jim Molan AO, DSC (LP, NSW) (from 05.02.2018)

Senator Murray Watt (ALP, QLD)

Former members

Senator David Fawcett (LP, SA) (until 05.02.2018)

Substituted members

Senator Jordon Steele-John (AG, WA) to replace Senator Nick McKim (AG, TAS)

Participating members

Senator Slade Brockman (LP, WA)

Senator Derryn Hinch (DHJP, VIC)

Senator Rex Patrick (NXT, SA)

Senator Linda Reynolds CSC (LP, WA)

Secretariat

Mr Tim Watling, Committee Secretary

Mr Antony Paul, Senior Research Officer

Ms Alexandria Moore, Administrative Officer

Suite S1.61	Telephone:	(02) 6277 3560
Parliament House	Fax:	(02) 6277 5794
CANBERRA ACT 2600	Email:	legcon.sen@aph.gov.au

Table of contents

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.

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.

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.

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.**

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.

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, and**
- **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.**

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.

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.

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.

Chapter 1

Introduction

1.1 On 7 September 2017 the Senate referred the following matter to the Legal and Constitutional Affairs References Committee (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.[1]

1.2 On 19 October 2017 the Senate extended the committee's reporting date to the last sitting day in March 2018.[2]

Conduct of this inquiry

1.3 Details of this inquiry were advertised on the committee's website, including a call for submissions to be received by 13 October 2017.[3] The committee continued to accept submissions after this deadline. The committee wrote directly to some organisations inviting them to make submissions. The committee received 34 submissions, of which three were received *in camera*. An attachment to one of the 34 submissions was also received *in camera*. The submissions are listed at appendix 1 of this report.

1.4 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. A list of witnesses who appeared at the hearings is available at appendix 2.

1.5 The committee thanks all those who made submissions or gave evidence at its public hearings. The committee gives particular thanks to those who gave evidence regarding the extreme effects of cyberbullying and online abuse on their lives.

---

1 *Proof Journals of the Senate*, No. 59, 7 September 2017, p. 1896.

2 *Proof Journals of the Senate*, No. 67, 19 October 2017, p. 2140.

3 The committee's website can be found at www.aph.gov.au/Parliamentary_Business/Committees/Senate/Legal_and_Constitutional_Affairs.

Structure of this report

1.6 There are 5 chapters in this report:

- This chapter provides information about the conduct of the inquiry as well as relevant background.
- Chapter 2 examines the nature and prevalence of cyberbullying.
- Chapter 3 considers the adequacy of existing criminal offences.
- Chapter 4 examines the policies, procedures and practices of social media platforms, as well as education and prevention initiatives.
- Chapter 5 provides the committee's view.

Background

1.7 The motion referring this matter to the committee was moved by former Senator Kakoschke-Moore.[4] The former senator stated that she moved the motion in response to the death of Libby Bell, a 13 year old girl who resided in South Australia.[5] Ms Bell committed suicide in August 2017 and her family has said that she suffered cyberbullying and physical bullying.

1.8 The problem of cyberbullying has received significant public attention.[6] In particular, the committee is aware of a number of youth suicides in recent years that were linked in the media, to at least some extent, with cyberbullying. One recent, high profile example is the suicide of 14 year old Amy "Dolly" Everett in January 2018.

1.9 The Council of Australian Governments (COAG) discussed cyberbullying at its meeting on 9 February 2018. The communique from that meeting stated:

> Bullying has no place in Australia, and can be especially harmful on children and young people. The growth of social media and mobile devices means that Australians can be subject to bullying 24 hours a day and from any location. Leaders heard from the eSafety Commissioner, Ms Julie Inman Grant, on initiatives to combat cyberbullying and acknowledged the ongoing importance of this work. First Ministers agreed that if we are to successfully reduce the incidence of bullying, we must better understand its underlying drivers and adopt a whole-of-community approach. COAG agreed that a working group of senior officials from First Ministers', Education, Justice and Health departments consider existing and potential initiatives to help combat bullying and cyberbullying and establish a work program to be led by the Education Council. The

4 *Proof Journals of the Senate*, No. 59, 7 September 2017, p. 1896.

5 Skye Kakoschke-Moore, 'Skye Kakoschke-Moore: Cyberbullying won't be solved quickly', *The Advertiser*, 2 October 2017, http://www.adelaidenow.com.au/news/opinion/skye-kakoschkemoore-cyberbullying-wont-be-solved-quickly/news-story/2234ab1b5af0257dfb2ea39750513c3f (accessed 13 December 2017).

6 See, for a recent example, Genevieve Gannon, 'Sticks and stones and mobile phones' *The Australian Women's Weekly*, March 2018, pp. 40–44.

> Education Council will report to COAG at its next meeting on tangible measures where there is an identified need.[7]

1.10 On 19 February 2018, the Queensland Government announced the formation of an anti-cyberbullying task force to make recommendations by 31 August 2018. The task force is chaired by Ms Madonna King, journalist and author.[8]

1.11 On 25 February 2018, it was reported that Minister for Education and Training, Senator the Hon. Simon Birmingham, stated:

> Following the discussion of bullying at COAG I have asked all state education ministers to bring examples of effective anti-bullying programs and the evidence that supports them to our next education council meeting.[9]

1.12 On 28 February 2018, the Prime Minister, the Hon. Malcolm Turnbull MP, and the Minister for Education and Training, Senator the Hon. Simon Birmingham, wrote to all school principals in Australia. Their letter stated: '[w]e encourage you and your school community to get involved in the National Day of Action against Bullying and Violence 2018', then upcoming on 16 March 2018.[10]

The eSafety Commissioner

1.13 The Children's eSafety Commissioner was established under the *Enhancing Online Safety Act 2015* (Online Safety Act) as an independent statutory office '…to take a national leadership role in online safety for children.'[11]

1.14 In June 2017 the Children's eSafety Commissioner's functions were expanded to include all Australians, not only Australian children.[12] Accordingly, the name was changed to the eSafety Commissioner. The broadened role of the eSafety Commissioner includes:

---

7 Council of Australian Governments, COAG meeting Communiqué, 9 February 2018, http://www.coag.gov.au/meeting-outcomes/coag-meeting-communiqu%C3%A9-9-february-2018 (accessed 26 February 2018).

8 The Hon. Annastacia Palaszczuk, Premier and Minister for Trade, 'Membership and terms of reference for Queensland Anti-Cyberbullying Task Force', *Media Statements*, 19 February 2018, http://statements.qld.gov.au/Statement/2018/2/19/membership-and-terms-of-reference-for-queensland-anticyberbullying-task-force (accessed 21 March 2018).

9 Senator the Hon. Simon Birmingham, Minister for Education and Training, in Lanai Scarr, 'Cyber-bullying epidemic: Australia falls behind in efforts to protect vulnerable kids', *Sunday Tasmanian*, 25 February 2018, p. 19.

10 Australian Government Department of Education and Training, answers to questions on notice, 7 March 2018 (received 16 March 2018), Attachment A.

11 Explanatory Memorandum, Enhancing Online Safety for Children Bill 2014 and Enhancing Online Safety for Children (Consequential Amendments) Bill 2014, pp. 1–2.

12 Enhancing Online Safety for Children Amendment Bill 2017.

> …functions in relation to persons at risk of family or domestic violence, in relation to victims of the non-consensual sharing of intimate images, and in relation to the safe use of the internet by older Australians.[13]

1.15 A key function of the eSafety Commissioner is to administer a complaints system for cyberbullying material targeting an Australian child.[14] The eSafety Commissioner stated that '[t]he scheme empowers the office to remove cyberbullying material that is posted online quickly. It is the only one of its kind in the world…'.[15]

1.16 However, the 2017 expansion did not extend the cyberbullying complaints scheme to adults; the scheme remains limited to cyberbullying material targeting an Australian child. The Explanatory Memorandum for the relevant bill explained:

> This is because while the Government recognises that online dangers such as cyber-bullying apply to both adults and children, there are existing avenues, including existing criminal laws, which apply to using the internet to menace and harass people of all ages.
>
> In our society, there are a range of areas where extra protections are put in place for children consistent with Australia's obligations under the [Convention on the Rights of the Child]. The Government considers child victims of cyber-bullying a priority.
>
> The Government does not consider there is any need to create any new powers to investigate cyberbullying complaints between adults at this time.[16]

1.17 Since the Office of the eSafety Commissioner (eSafety Office) was established in July 2015, '…the Commissioner has resolved approximately 550 complaints in relation to cyberbullying material.'[17] Between 1 October 2017 and 31 January 2018, cyberbullying complaints to the eSafety Office increased by 30% compared to the same period 12 months prior.[18] In addition, the eSafety Office has referred approximately 6,000 young Australians to the Kids Helpline.[19] The committee notes that it is plausible that there are many more cases of cyberbullying than indicated by these figures, as many cases would not be reported to the eSafety Commissioner.

---

13 Explanatory Memorandum, Enhancing Online Safety for Children Amendment Bill 2017, p. 2.

14 Explanatory Memorandum, Enhancing Online Safety for Children Bill 2014 and Enhancing Online Safety for Children (Consequential Amendments) Bill 2014, p. 2; Office of the eSafety Commissioner (eSafety Office), *Submission 13*, p.4.

15 Ms Julie Inman Grant, eSafety Commissioner, eSafety Office, *Committee Hansard*, 9 February 2018, p. 61.

16 Explanatory Memorandum, Enhancing Online Safety for Children Amendment Bill 2017, p. 9.

17 eSafety Office, *Submission 13*, p. 2.

18 eSafety Office, answers to questions on notice, 9 February 2018 (received 7 March 2018), p. 2.

19 Ms Inman Grant, eSafety Commissioner, *Committee Hansard*, 9 February 2018, p. 64.

1.18 The eSafety Office manages these cyberbullying cases, and its other work, with a staff of approximately 78 and a budget of about $17 million per annum. The team that deals with cyberbullying complaints is comprised of four staff.[20]

The tier scheme for cyberbullying complaints

1.19 The Online Safety Act '…establishes a two-tiered scheme for the rapid removal from social media services of cyberbullying material targeted at an Australian child.'[21] The eSafety Office explained that:

> [a] social media service can apply to the Commissioner to be declared a Tier 1 social media service. To be declared a Tier 1 service, the Commissioner must be satisfied that the social media service meets certain basic online safety requirements.[22]

1.20 These safety requirements include that the platform have terms of use that prohibit cyberbullying, that it provide a clear complaints process for users, and that it designate a contact person to liaise with the eSafety Office for the purposes of the Online Safety Act.[23]

1.21 The eSafety Commissioner can issue a notice requesting that a Tier 1 service remove cyberbullying material within 48 hours:

> Non-compliance with a notice by a Tier 1 service does not attract a legal penalty. However, if a Tier 1 service repeatedly fails to comply with a request to remove material, or if it no longer complies with the Act's basic online safety requirements under section 21 of the Act, the Commissioner can revoke its tier 1 status.
>
> The Commissioner may also publish a statement on the Commissioner's website to the effect that a Tier 1 social media service has failed to remove material when requested.[24]

1.22 A social media service may be declared as Tier 2 by the minister on recommendation from the eSafety Commissioner. To make such a recommendation, the eSafety Commissioner '…must be satisfied that the service is a "large social media service", or that the service has *requested* to be a Tier 2 service.'[25]

1.23 Tier 2 services are '… subject to somewhat more interventionist measures.'[26] The eSafety Commissioner may issue a Tier 2 service with a notice requiring the

---

20 Ms Inman Grant, eSafety Commissioner, and Mr Toby Dagg, Acting Manager, Compliance Tools and Citizen Services, eSafety Office, Committee Hansard, 9 February 2018, p. 73.

21 eSafety Office, *Submission 13*, p. 4.

22 eSafety Office, *Submission 13*, p. 5.

23 eSafety Office, *Submission 13*, p. 4; Mr Dagg, eSafety Office, *Committee Hansard*, 9 February 2018, p. 63.

24 eSafety Office, *Submission 13*, p. 5.

25 eSafety Office, *Submission 13*, p. 5.

26 Mr Dagg, eSafety Office, *Committee Hansard*, 9 February 2018, p. 63.

service to remove cyberbullying material within 48 hours. However, the material must have first been reported to the service by a user, and 48 hours must have elapsed since that time. If a Tier 2 service does not comply with a notice then enforcement action may be taken.[27]

1.24 This tier scheme was summarised by the eSafety Office follows:

> Basically, the tier 1 scheme is an opt-in scheme, so a company can volunteer. However, in the instances where we've identified that a lot of cyberbullying is occurring on a particular site and we've invited them to become tier 1 but they didn't elect to take up that offer or invitation, we can declare them or recommend that they be declared tier 2, which, in turn, gives us more enforcement power.[28]

1.25 Currently, the social media services declared as Tier 1 are: airG, Ask.fm, Snapchat, Twitter, Yahoo!7 Answers, and Yahoo!7 Groups. The services declared as Tier 2 are: Facebook, Google+, Instagram, and Youtube.[29]

The eSafety Commissioner's discretionary powers

1.26 The eSafety Commissioner has '…a broad range of discretionary powers and civil penalties…'.[30] The eSafety Commissioner stated that:

> [t]his includes fines of up to $18,000 a day for tier 2 social media sites that do not comply with our take-down notices. While this might be pocket change for some of the behemoths, using our position to name and shame, and to make a reputational impact, cannot be underestimated.[31]

1.27 The eSafety Commissioner has not yet used its formal powers or issued any civil penalties as it has not yet considered this to be appropriate.'[32]

1.28 The eSafety Commissioner may also issue an end-user notice to an individual person who posted cyberbullying material, requiring them to:

- take all reasonable steps to ensure the removal of the material;
- refrain from posting any cyberbullying material targeting a child, or
- apologise for posting the material.[33]

---

27 eSafety Office, *Submission 13*, p. 5; Ms Inman Grant, eSafety Commissioner, *Committee Hansard*, 9 February 2018, p. 62.

28 Ms Maria Vassiliadis, Executive Manager, eSafety Office, *Committee Hansard*, 9 February 2018, p. 63.

29 eSafety Office, *Submission 13*, p. 6.

30 Ms Inman Grant, eSafety Commissioner, *Committee Hansard*, 9 February 2018, p. 61.

31 Ms Inman Grant, eSafety Commissioner, *Committee Hansard*, 9 February 2018, p. 61.

32 Ms Inman Grant, eSafety Commissioner, and Mr Dagg, eSafety Office, *Committee Hansard*, 9 February 2018, p. 64.

33 eSafety Office, *Submission 13*, p.6.

1.29 The eSafety Office submitted that it '…recognise[s] the need to be proportionate and balanced in how discretionary powers might be used to deal with cyberbullying', particularly where the cyberbullying material was posted by a child.[34]

1.30 The eSafety Office stated that it has not yet issued any end-user notices:

> To date, the cases handled by the Office have not warranted such an intervention. Each has been resolved through the 'hybrid' approach of taking the material down quickly whilst also working with schools, parents and victims.[35]

Australian Cybercrime Online Reporting Network

1.31 The Australian Cybercrime Online Reporting Network (ACORN) is:

> …a national policing initiative of the Commonwealth, State and Territory governments. It is a national online system that allows the public to securely report instances of cybercrime. It will also provide advice to help people recognise and avoid common types of cybercrime.[36]

1.32 The ACORN was '…a key initiative under the 2013 *National Plan to Combat Cybercrime*.'[37] The ACORN's website lists cyberbullying as a type of cybercrime.[38]

Existing policies and legislation

1.33 The committee heard evidence about polices and legislation that relate to cyberbullying both in Australia and overseas.[39]

Australia

1.34 In general, Commonwealth offences that could apply to cyberbullying relate to the misuse of carriage services. These offences are examined in greater detail in Chapter 3.

1.35 State and territory criminal offences that could apply to cyberbullying vary between jurisdictions. Generally speaking, there are a variety of offences in each jurisdiction that could apply to cyberbullying behaviours. These offences tend to relate

---

34 eSafety Office, *Submission 13*, p.6.

35 eSafety Office, *Submission 13*, p.7.

36 Australian Cybercrime Online Reporting Network (ACORN), 'About the ACORN', https://www.acorn.gov.au/about-acorn (accessed 19 March 2018).

37 Attorney-General's Department, 'Cybercrime', https://www.ag.gov.au/CrimeAndCorruption/Cybercrime/Pages/default.aspx (accessed 19 March 2018).

38 ACORN, 'Learn about cybercrime', https://www.acorn.gov.au/learn-about-cybercrime (accessed 19 March 2018).

39 See, for example, eSafety Commissioner, answers to questions on notice, 9 February 2018 (received 7 March 2018).

to stalking, harassment, assault, threats, and defamation.[40] Some examples of specific offences are as follows:

- Section 60E of the *Crimes Act 1900* (New South Wales) contains '…a criminal provision for bullying which makes it an offence to assault, stalk, harass or intimidate any school student or member of staff of a school while the student or member of staff is attending a school.'[41] The maximum penalty ranges from five to 12 years' imprisonment depending on the severity of the offence. While this provision could apply to cyberbullying, '…the necessary act must take place at a school', thereby limiting the application of the offence.[42]
- Part 5A of the *Summary Offences Act 1953* (South Australia) includes a range of offences relating to cyberbullying and the non-consensual sharing of intimate images. This includes offences against humiliating or degrading filming, distribution of an invasive image, indecent filming, and threatening to distribute invasive images.[43]
- "Brodie's Law" in Victoria makes serious bullying a criminal offence by extending '…the definition of stalking in section 21A of the *Crimes Act 1958* (Vic) to specifically include behaviour that could lead a person to self-harm.'[44] The offence is punishable by up to 10 years' imprisonment, and could apply to serious cyberbullying.[45] The offence was introduced following the passage of the Crimes Amendment (Bullying) Bill 2011 in June 2011. It is known as "Brodie's Law", named after Ms Brodie Panlock who committed suicide in 2006 at age 19 after suffering bullying in her workplace.

Non-consensual sharing of intimate images

1.36 The committee heard evidence relating to the non-consensual sharing of intimate images as a further type of cyberbullying.[46] In May 2017 all Australian jurisdictions agreed, through the Law, Crime and Community Safety Council, to the

40 For listings of specific legislative provisions, see Australian Universities' Anti-bullying Research Alliance, *Submission 1*, pp. 5–6; Law Council of Australia, *Submission 15*, p. 11.

41 Mental Health Commissions of Australia, *Submission 9*, pp. 4–5.

42 Mental Health Commissions of Australia, *Submission 9*, p. 5.

43 South Australian Government, *Submission 21*, pp. 2–5.

44 Mental Health Commissions of Australia, *Submission 9*, p. 3.

45 Victoria State Government Justice and Regulation, *Bullying – Brodie's Law*, http://www.justice.vic.gov.au/home/safer+communities/crime+prevention/bullying+-+brodies+law (accessed 20 December 2017).

46 See, for example, Instagram, *Submission 3*, p. 3; Facebook, *Submission 4*, p. 4; Western Australia Police Force, *Submission 11*, p. 2; Australian Women Against Violence Alliance, *Submission 14*, p. 2; South Australian Government, *Submission 21*, p. 8;

National Statement of principles relating to the criminalisation of the non-consensual sharing of intimate images.[47] These principles are non-binding and state:

> This document identifies best practice principles to be considered as each jurisdiction continues to develop and review its criminal law, policy and practices to suit local needs, and for each jurisdiction to adopt and implement as that jurisdiction sees fit.[48]

1.37 Most Australian states and territories have introduced offences that specifically relate to the non-consensual sharing of intimate images.[49]

1.38 On 6 December 2017 the Enhancing Online Safety (Non-consensual Sharing of Intimate Images) Bill 2017 was introduced into the Senate by the Assistant Minister to the Prime Minister, Senator the Hon. James McGrath. The bill would introduce a civil penalty regime for the non-consensual sharing of intimate images, with penalties of up to $105,000 for an individual and $525,000 for a body corporate. The regime would be administered by the eSafety Commissioner.

1.39 The bill passed the Senate with amendments on 14 February 2018.[50] The bill was amended to:

- require the minister to cause an independent review of the operation of the bill to be conducted within three years, and to table a copy of the review's report in parliament; and
- introduce criminal offences relating to the non-consensual sharing of intimate images.

1.40 At the time of writing, the bill is before the House of Representatives.

Harmful Digital Communications Act 2015 (New Zealand)

1.41 Some submitters referred to New Zealand's *Harmful Digital Communications Act 2015* (Harmful Communications Act) as potentially useful for considering reform in Australia.[51]

---

47 Communique, Law, Crime and Community Safety Council, 19 May 2017, https://www.ag.gov.au/About/CommitteesandCouncils/Law-Crime-and-Community-Safety-Council/Documents/19-May-LCCSC-Communique.pdf (accessed 5 February 2018).

48 National statement of principles relating to the criminalisation of the non-consensual sharing of intimate images, Law, Crime and Community Safety Council, https://www.ag.gov.au/CrimeAndCorruption/Cybercrime/Documents/National-statement-of-principles-criminalisation-non-consensual-sharing-intimate-images.PDF (accessed 5 February 2018).

49 Terry Goldsworthy, 'Revenge porn laws may not be capturing the right people', *The Conversation*, 29 September 2017, https://theconversation.com/revenge-porn-laws-may-not-be-capturing-the-right-people-84061 (accessed 13 March 2018).

50 *Proof Journals of the Senate*, No. 86, 14 February 2018, p. 2714.

51 See, for example, National Council of Single Mothers & their Children, *Submission 7*, p. 2; Alannah & Madeline Foundation, *Submission 10*, p. 6; Media, Entertainment & Arts Alliance, *Submission 28*, p. 7; Maurice Blackburn Lawyers, *Submission 29*, p. 5

1.42 Key features of the Harmful Communications Act include the following:[52]

- Making it a criminal offence to '…post a digital communication with the intention that it cause harm to a victim…', where posting the communication harmed the victim and would have caused harm '…to an ordinary reasonable person in the position of the victim…'.[53] The offence is punishable by up to two years' imprisonment or a maximum fine of $50,000 for individuals or $200,000 for companies.
- Establishing an approved agency to resolve complaints about harmful digital communications. NetSafe has been appointed as the approved agency.
- Enabling a court to hear civil proceedings about serious or repeated harmful digital communications. The court does not issue fines or prison terms, but can order certain remedies. Failure to comply with these orders is punishable by up to six months' imprisonment or a fine of $5,000 for individuals or $20,000 for companies. The court is able '…to order a broad range of remedies…', which include:
  - orders to take down material;
  - cease-and-desist orders;
  - orders to publish a correction or an apology, or to give the complainant a right of reply;
  - orders to release the identity of the source of an anonymous communication, and
  - ordering name suppression for any parties.[54]
- Limiting the liability of telecommunications companies and social media platforms for harmful content posted by others, as long as those companies follow a certain procedure for users' complaints.
- Making it a criminal offence to incite someone to commit suicide, regardless of whether or not the person attempts suicide (previously, it was only an offence if the person attempted or committed suicide). The offence is punishable by up to three years' imprisonment.

1.43 During his second reading speech on the bills that established the Australian eSafety Commissioner, the then Parliamentary Secretary to the Minister for

52 New Zealand Ministry of Justice, 'Key parts of the Act', 2 October 2017, https://www.justice.govt.nz/justice-sector-policy/key-initiatives/harmful-digital-communications/key-parts-of-the-act/ (accessed 19 March 2018).

53 *Harmful Digital Communications Act 2015* (New Zealand), subsection 22(1).

54 New Zealand Ministry of Justice, 'Key parts of the Act', 2 October 2017, https://www.justice.govt.nz/justice-sector-policy/key-initiatives/harmful-digital-communications/key-parts-of-the-act/ (accessed 19 March 2018).

Communications, the Hon. Paul Fletcher MP, referred to various elements of the Harmful Communications Act that had been considered.[55]

Network Enforcement Law in Germany

1.44 The Netzwerkdurchsetzungsgesetz (also known as NetzDG or Network Enforcement Law) places various obligations on social media platforms in Germany. It was passed in June 2017 and came into force in early October 2017, although there was a transition period until 1 January 2018.[56]

1.45 The Network Enforcement Law applies to social media platforms that have over two million registered users in Germany.[57] It requires the platforms to block or remove access to:

- 'manifestly unlawful content' within 24 hours of receiving a complaint, and
- 'unlawful content' within seven days of receiving a complaint.[58]

1.46 The meaning of 'unlawful content' is limited to content that contravenes certain enumerated criminal offences. These offences include those relating to hate speech, inciting others to violence or crime, terrorist offences, glorifying violence, defamation, insult, and child pornography.[59]

1.47 The Network Enforcement Law also requires social media platforms to:

- maintain an effective procedure for users to make complaints about content;[60]
- publish half-yearly reports providing certain specified data relating to the implementation of the law,[61] and
- name and authorise a person to receive service in Germany.[62]

---

55 The Hon. Paul Fletcher MP, Parliamentary Secretary to the Minister for Communications, *House of Representatives Hansard*, 3 December 2014, p. 14039.

56 'Germany starts enforcing hate speech law', *BBC News*, 1 January 2018, http://www.bbc.com/news/technology-42510868 (accessed 19 March 2018).

57 Network Enforcement Act (English translation), subsection 1(1), https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf?__blob=publicationFile&v=2 (accessed 19 March 2018).

58 Network Enforcement Act (English translation), subsection 3(2), https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf?__blob=publicationFile&v=2 (accessed 19 March 2018).

59 Network Enforcement Act (English translation), subsection 1(3), https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf?__blob=publicationFile&v=2 (accessed 19 March 2018).

60 Network Enforcement Act (English translation), subsections 2(1) and (2), https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf?__blob=publicationFile&v=2 (accessed 19 March 2018).

61 Network Enforcement Act (English translation), subsection 1(1), https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf?__blob=publicationFile&v=2 (accessed 19 March 2018).

1.48 Failing to meet the requirements of the Network Enforcement Law can result in fines of up to 50 million euros.[63]

USA Communications Decency Act 1996

1.49 The eSafety Commissioner explained that legislation in the United States of America '…has given the social media sites what is called intermediary liability—what I believe some of them now call intermediary immunity—which says that they're not responsible for anything that users do on their platform.'[64] This is under the *Communications Decency Act 1996*, of which subsection 230(c)(1) states that:

> No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.[65]

Note on references

1.50 In this report, references to *Committee Hansard* are to proof transcripts. Page numbers may vary between proof and official transcripts.

62 Network Enforcement Act (English translation), section 5, https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf?__blob=publicationFile&v=2 (accessed 19 March 2018).

63 Ben Knight, 'Germany implements new internet hate speech crackdown', *Deutsche Welle*, 1 January 2018, http://www.dw.com/en/germany-implements-new-internet-hate-speech-crackdown/a-41991590 (accessed 19 March 2018); Philip Oltermann, 'Tough new German law puts tech firms and free speech in spotlight', *The Guardian*, 5 January 2018, https://www.theguardian.com/world/2018/jan/05/tough-new-german-law-puts-tech-firms-and-free-speech-in-spotlight (accessed 19 March 2018).

64 Ms Inman Grant, eSafety Commissioner, *Committee Hansard*, 9 February 2018, p. 71.

65 *Communications Decency Act 1996* (USA), Subsection 230(c)(1), in eSafety Office, answers to questions on notice, 9 February 2018 (received 7 March 2018), p. 3.

Chapter 2

What is cyberbullying?

2.1 Cyberbullying, like other forms of bullying, can cause severe harm to the victim and to others around them.

2.2 Many submitters emphasised that cyberbullying is a complex problem.[1] As Professor Marilyn Campbell, Founding Member of the Australian Universities' Anti-bullying Research Alliance (AUARA) argued, '…all forms of bullying are a very complex problem. As such, they are deeply embedded in our society, and you can't have one simple solution for such a complex problem.'[2]

2.3 Moreover, cyberbullying can occur in many forms and contexts. As the Tasmanian Government submitted:

> Cyberbullying covers a broad range of conduct, relationships, motivations and means of distribution. Cyberbullying can be used to coerce, control, abuse, blackmail, humiliate, intimidate or harass another person.[3]

2.4 The wide-ranging nature of cyberbullying was demonstrated by the breadth of evidence received by the committee. In particular, the committee heard that cyberbullying between children is often very different to cyberbullying targeting adults, although the two are not entirely distinct.

2.5 This chapter outlines evidence received by the committee regarding:

- the nature of cyberbullying between children;
- the nature of cyberbullying targeting adults, and
- working toward a consistent and national definition of cyberbullying.

Cyberbullying between children

The prevalence of cyberbullying between children

2.6 The Tasmanian Government highlighted that '[t]he use of modern technology has contributed to the prevalence of cyberbullying and the ease with which a person can access and distribute offensive material.'[4]

2.7 The Office of the eSafety Commissioner (eSafety Office) stated that approximately one in five Australian children are cyberbullied.[5] The eSafety Office also provided data from its research, which indicate that:

---

1 See, for example, Australian Universities Anti-bullying Research Alliance (AUARA), *Submission 1*, p. 6; Office of the eSafety Commissioner (eSafety Office), *Submission 13*, p. 1; Tasmanian Government, *Submission 19*, p. 2;

2 Professor Marilyn Campbell, Founding Member, AUARA, *Committee Hansard*, 9 February 2018, p. 1.

3 Tasmanian Government, *Submission 19*, p. 2.

4 Tasmanian Government, *Submission 19*, p. 2.

> [i]n the 12 months to June 2016, 8% of children and 19% of teenagers were cyberbullied, and we saw a 63% increase in complaints about cyberbullying between 2015-16 and 2016-17.
>
> Further, research indicates that girls are cyberbullied more frequently than boys, although an increasing number of boys were targets over 2016-17.[6]

2.8 In addition, the eSafety Commissioner, Ms Julie Inman Grant, recently said that '[w]e have seen a 133 per sent spike in cyberbullying reports from young people over the first two weeks of February when kids have been going back to school.'[7]

2.9 yourtown cited figures from the Kids Helpline, stating that:

> [i]n 2017 alone, Kids Helpline had over 3,000 contacts about cybersafety, with over 950 contacts concerned about cyberbullying. A significant proportion of these—some 44 per cent—were made by children aged only 12 to 14, revealing that cyberbullying is common in transitional years between primary and secondary school and during puberty.[8]

2.10 Moreover, '[Kids Helpline] tip sheets on cyberbullying issues were viewed 23,183 times in 20l6, with 7,226 accessing parent and teacher tip sheets on the issue.'[9]

2.11 The Queensland Family and Child Commission submitted that cyberbullying is most prominent among young people aged 10–15 years.[10] Mr Jeremy Blackman, Senior Advisor, Cybersafety at the Alannah & Madeline Foundation, stated that cyberbullying can be particularly high around 'transition to secondary school'.[11]

2.12 Although these figures show cyberbullying to be fairly widespread, the committee heard that it is merely one type of bullying.[12] Professor Campbell of AUARA highlighted that '[f]ace-to-face bullying is shown still to be much more prevalent than cyberbullying. We really need to look at the problem as a whole.'[13]

2.13 The Queensland Family and Child Commission also submitted that measures against cyberbullying 'should take into account the increased vulnerability of some

---

5 eSafety Office, answers to questions on notice, 9 February 2018 (received 7 March 2018); also see, for example, yourtown, *Submission 6*, p. 4; Tasmanian Government, *Submission 19*, p. 2.

6 eSafety Office, *Submission 13*, p. 2.

7 Ms Julie Inman Grant, eSafety Commissioner, in Jake Evans, 'Fake Instagram accounts being used by kids to "destroy reputations", eSafety Commissioner says', *ABC News*, 16 March 2018, http://www.abc.net.au/news/2018-03-16/children-using-fake-instagram-accounts-to-bully-others/9553548 (accessed 16 March 2018).

8 Ms Laura Clarke, Advocacy and Policy Lead, yourtown, *Committee Hansard*, 9 February 2018, pp. 20–21.

9 yourtown, *Submission 6*, p. 5.

10 Queensland Family and Child Commission, *Submission 8*, p. 2.

11 Mr Jeremy Blackman, Senior Advisor, Cybersafety, Alannah & Madeline Foundation, *Committee Hansard*, 9 February 2018, p. 23.

12 Professor Campbell, AUARA, *Committee Hansard*, 9 February 2018, p. 4.

13 Professor Campbell, AUARA, *Committee Hansard*, 9 February 2018, p. 6.

groups of children, including girls, Aboriginal and Torres Strait Islander children, children with a disability and children with cognitive impairments.'[14]

Causes of cyberbullying between children

2.14 Many submitters argued that cyberbullying between children is linked with other bullying, often within the school environment.[15] The Attorney-General's Department called cyberbullying '…a modern manifestation of "traditional" bullying behaviour.'[16] Similarly, the eSafety Office stated that:

> [i]n many instances, cyberbullying is an extension of bullying or conflict occurring within the school. In reports to eSafety about cyberbullying, victims often note that the harassment they experience online mirrors their experience at school. Further, the perpetrators are in many instances the same.[17]

2.15 Mr John Dalgleish, Head of Strategy and Research at yourtown, explained:

> In our data, what 400 young people have said to us in the last week is that 85 per cent knew who was cyberbullying and two-thirds of those who were being cyberbullied knew that it was the bully that was doing it in a face-to-face situation.[18]

2.16 The Australian Human Rights Commission submitted that children tend not to distinguish between the physical and digital world:

> Consultations with children by the National Children's Commissioner reveal that most children do not see a clear distinction between the online and physical world and report that bullying usually occurs in both physical and online settings.[19]

2.17 Mr Dalgleish of yourtown also explained that '…from our research and our service experiences, a child can be bullied, be the bully and be a bystander to bullying at any time in their life.'[20] Ms Lesley Podesta, Chief Executive Officer of the Alannah & Madeline Foundation, provided some data on this point:

---

14 Queensland Family and Child Commission, *Submission 8*, pp. 2–3.

15 See, for example, Queensland Family and Child Commission, *Submission 8*, p. 2; Mental Health Commissions of Australia, *Submission 9*, p. 2

16 Attorney-General's Department, *Submission 20*, p. 4.

17 eSafety Office, *Submission 13*, p. 3; also see, for example, Queensland Family and Child Commission, *Submission 8*, p. 2; Mental Health Commissions of Australia, *Submission 9*, p. 2; Professor Campbell, AUARA, *Committee Hansard*, 9 February 2018, p. 4.

18 Mr John Dalgleish, Head of Strategy and Research, yourtown, *Committee Hansard*, 9 February 2018, p. 26.

19 Australian Human Rights Commission, *Submission 16*, p. 2.

20 Mr Dalgleish, yourtown, *Committee Hansard*, 9 February 2018, p. 22.

> …there are nearly 900,000 bullying incidents of children in Australia a year. Approximately one-third of those are children who are victims and perpetrators. There's a significant crossover between the groups.[21]

2.18 Dr Kerrie Buhagiar, Director of Service Delivery at ReachOut Australia, posited a reason for cyberbullying having become normalised among young people:

> I think the primary reason is the prevalence, because they see it happening all around them in their everyday lives, online and offline. So, it has I guess become perceived as a normal part of teenage behaviour.[22]

2.19 Mr Blackman of the Alannah & Madeline Foundation stated that bullying behaviours are '…generally recognised as a learned behaviour' and also that '…the trauma of going through bullying or cyberbullying can, in many cases, lead to that person becoming a perpetrator of that same behaviour.'[23]

2.20 Ms Laura Clarke, Advocacy and Policy Lead at yourtown, posited that, given the cyberbullying conducted by adults, children who cyberbully '…can simply be seen to be modelling the behaviour of their elders and the wider community.'[24] yourtown also provided several case studies of cyberbullying perpetrators contacting the Kids Helpline, and explained that '…young cyberbullies can be motivated to bully for a series of reasons…',[25] including:[26]

- for fun or entertainment, as a joke, or because they are bored;
- because they feel powerless, unheard, or frustrated, and cyberbullying is a way to get attention or vent their anger;
- because they see others doing it, wish to model others' behaviour, or feel peer pressure;
- to maintain their popularity; or
- because they may have been a victim of cyberbullying themselves and are seeking justice.

2.21 Further, yourtown argued that '…an important element of cyberbullying is the nature of the internet', and submitted that:

> [t]he internet can be seen to facilitate bullying or be an unwieldy, powerful tool with far-reaching repercussions in the hands of witting or unwitting bullies given that:

---

21 Ms Lesley Podesta, Chief Executive Officer, Alannah & Madeline Foundation, *Committee Hansard*, 9 February 2018, p. 22.

22 Dr Kerrie Buhagiar, Director of Service Delivery, ReachOut Australia, *Committee Hansard*, 7 March 2018, p. 30.

23 Mr Blackman, Alannah & Madeline Foundation, *Committee Hansard*, 9 February 2018, p. 23.

24 Ms Clarke, yourtown, *Committee Hansard*, 9 February 2018, p. 21.

25 yourtown, answers to questions on notice, 9 February 2018 (received 16 February 2018), p. 3.

26 yourtown, answers to questions on notice, 9 February 2018 (received 16 February 2018), pp. 3–4.

- People can post anonymously, freeing people's normal inhibitions so that they feel they can say whatever they like without consequence
- People feel less empathy or concerned by their actions as they cannot see the hurt that they are causing their friend or stranger
- Complete strangers can cast their opinion on people's posts or pictures, about whom they have no personal knowledge, connection and therefore as a result, no empathy with the individual they may be attacking
- Posts online can be shared to an audience of thousands, and once online, posts can be re-shared and have long-lasting and ongoing effects
- Bullies can now reach their targets in their own homes 24/7, victims cannot escape even at home and even if they come off social media as they can receive personal texts.[27]

Cyberbullying behaviours between children

2.22 The eSafety Office submitted that:

> [t]he most common forms of cyberbullying are social exclusion, name calling, and the spreading of lies and malicious rumours. Our experience shows that children and teens are predominantly bullied online by those in their own peer group.[28]

2.23 The Alannah & Madeline Foundation noted that '[t]he rapidly changing nature of technology means that the form cyberbullying takes continues to morph as new ways and means of using technology emerge.'[29] yourtown listed various types of cyberbullying behaviours:[30]

- harassment: repeatedly sending offensive messages to a target;
- cyberstalking: intense harassment and denigration that includes threats or creates significant fear in the victim (harassment becomes cyberstalking when a victim fears for their personal safety);
- denigration: making derogatory comments about a target. This can occur using words or can involve the dissemination of a derogatory, sexual or non-sexual image;
- happy slapping: the filming of a physical assault on a victim and the subsequent distribution of the film to humiliate the victim publically;

27 yourtown, answers to questions on notice, 9 February 2018 (received 16 February 2018), p. 2.

28 eSafety Office, *Submission 13*, p. 2.

29 Alannah & Madeline Foundation, *Submission 10*, p. 5.

30 yourtown, *Submission 6*, pp. 6–8; also see, for example, Law Council of Australia, *Submission 15*, p. 7.

- exclusion: purposely excluding a victim from entering online domains such as a chat room discussion group;
- outing and trickery: situations where a perpetrator manipulates the victim into disclosing information that the perpetrator then publicises in order to humiliate the victim; and
- impersonation or masquerading: where a perpetrator pretends to be the victim and sends offensive messages to others that appear to come from the victim.

2.24 The eSafety Commissioner has reported that the use of fake accounts to impersonate peers makes up '…about 20 per cent of our complaints.'[31]

2.25 Professor Campbell of AUARA stated that most cyberbullying between children is not anonymous. She said that the notion of anonymous cyberbullying:

> …is an adult perception because of trolling of adults, but kids usually only bully people that they know. So they don't troll and just be angry at celebrities; what they do is they pick on the kids at school and then, after they leave school, they send them horrible messages when they get home as well. So they usually know them. There's a very small percentage of kids who don't know them.[32]

2.26 While noting the overlap between cyberbullying and other bullying, some submitters highlighted differences between these two behaviours. The eSafety Commissioner stated that:

> I think what you saw with the whole idea of COAG coming together today is that state, territory and federal leaders said, 'Hey, bullying isn't a new phenomenon.' I heard the senator say that these are social and behavioural problems playing out in the technological sphere. I absolutely agree. There are some unique characteristics of cyberbullying vis-a-vis bullying. It's much more pervasive. Sometimes anonymity can be involved. With the amplification with multiple people watching or partaking, that can amplify a person's humiliation. With image based abuse and the fast proliferation of images, that's obviously a devastating impact for victims.[33]

2.27 The Tasmanian Government also distinguished between cyberbullying and traditional bullying:

> Cyberbullying differs somewhat from what is considered to be 'traditional' bullying in that it may involve a single but widely disseminated or indefinitely accessible communication rather than a sustained course of conduct. For example, where an online post is accessible indefinitely or the

---

31 Ms Inman Grant, eSafety Commissioner, in Jake Evans, 'Fake Instagram accounts being used by kids to "destroy reputations", eSafety Commissioner says', *ABC News*, 16 March 2018, http://www.abc.net.au/news/2018-03-16/children-using-fake-instagram-accounts-to-bully-others/9553548 (accessed 16 March 2018).

32 Professor Campbell, AUARA, *Committee Hansard*, 9 February 2018, p. 6.

33 Ms Julie Inman Grant, eSafety Commissioner, Office of the eSafety Commissioner, *Committee Hansard*, 9 February 2018, pp. 67–68.

> sharing of a post goes 'viral' on social media outlets reaching a large number of people.[34]

2.28 Similarly, yourtown submitted that '[o]nce bullying behaviour has been committed online, repetitive bullying is no longer solely at the instigation of the original bully or bullies.'[35]

2.29 yourtown also argued that '…evidence suggests that the detrimental impact of cyberbullying can be more severe and long lasting to its victims than traditional bullying.'[36] It explained:

> It is thought that cyberbullying can do more harm due to its wider reach – with cyberbullies having access to a global audience – and due to the facts that it no longer remains in the playground but can occur in the safety of victims own homes, can take place 24/7, be carried out anonymously and can remain on line in a number of different forums and be repeatedly relived.[37]

The effects of cyberbullying between children

2.30 The Australian Government Department of Education and Training highlighted the harms of cyberbullying:

> There is increasing evidence that both face-to-face bullying and cyberbullying have lasting effects on young people, including poor self-esteem and mental health, depression, anxiety and suicidal ideation. Recent tragic events have further generated widespread concern about the issue of cyberbullying.[38]

2.31 The Tasmanian Government stated that '[t]he harm caused by bullying can be very victim-specific and the consequences vary widely depending on the victim.'[39] yourtown painted a detailed picture of the negative effects cyberbullying can have:

> Callers contact Kids Helpline expressing high levels of anxiety, depression, isolation, humiliation or shame about cyberbullying. They tell us that they don't want to go to school, that their grades are deteriorating, that their relationships with their families and others are suffering and that they're no longer interested in the hobbies they used to enjoy. They feel hopeless, powerless and, most tragically, sometimes even suicidal. Indeed, some 14 per cent of young people who contacted our counsellors about online safety issues in 2017 were experiencing suicidal thoughts at the time of contact. Of notable concern, nine per cent of those were aged just five to 12 years old. We know therefore that cyberbullying is an increasingly prevalent issue, taking a serious emotional toll on the very youngest

---

34 Tasmanian Government, *Submission 19*, p. 2.

35 yourtown, *Submission 6*, p. 4.

36 yourtown, *Submission 6*, p. 4.

37 yourtown, *Submission 6*, p. 4.

38 Australian Government Department of Education and Training, *Submission 2*, p. 4.

39 Tasmanian Government, *Submission 19*, p. 2.

> Australians, with long-lasting and, at times, devastating consequences for the health and wellbeing of our children.[40]

2.32 In addition to victims, perpetrators can also be negatively affected by cyberbullying. yourtown stated that Kids Helpline hears from:

> …cyberbullies who ring us severely distressed, remorseful and worried about their future. These young cyberbullies urgently need appropriate support and education to help them more positively navigate their online worlds, including mental health support services targeted to meet their specific needs.[41]

2.33 The eSafety Office noted that the harms of cyberbullying extend even beyond victims and perpetrators:

> The consequences are often felt well beyond the perpetrator and victim involved, impacting families, friends and local communities. Schools are often adversely impacted, as are service providers such as out of home care organisations. In some cases, police become involved.[42]

2.34 Some submitters questioned the extent of any *direct* link between cyberbullying and suicide. The National Mental Health Commission stated:

> The real-world consequences of bullying in children and young people include the risk of developing a mental health condition, including either depression or anxiety, or both, and it can also lead to an increased risk of the use of drugs and alcohol as well as self-harm, suicidal ideation and suicide attempts.
>
> However, we do know that suicide is multifaceted, and its causes are complex…Research suggests that most people who die by suicide have underlying risk factors including mental health issues and other social influences.[43]

2.35 The National Children's Commissioner at the Australian Human Rights Commission, Ms Megan Mitchell, referred to research she conducted in 2014 which:

> …found that while bullying was a feature in some of the suicides of children it was rarely the sole factor at play. A multiplicity of risk factors predispose a child to suicide or self-harm. These include, as has been said, mental health problems, substance abuse, child abuse, adverse family experiences, school, stress, body image and a history of intentional self-harm with or without suicidal intent.[44]

---

40 Ms Clarke, yourtown, *Committee Hansard*, 9 February 2018, p. 21.

41 yourtown, answers to questions on notice, 9 February 2018 (received 16 February 2018), p. 4.

42 eSafety Office, *Submission 13*, p. 1.

43 Ms Vanessa D'Souza, Acting Director, Policy, Analysis and Reporting, National Mental Health Commission, *Committee Hansard*, 9 February 2018, p. 53.

44 Ms Megan Mitchell, National Children's Commissioner, Australian Human Rights Commission, *Committee Hansard*, 9 February 2018, p. 54.

2.36 Dr Buhagier of ReachOut Australia discussed the link between cyberbullying and mental distress, and the link between mental distress and suicide:

> The research that we've done with young people would suggest that cyberbullying actually is very closely linked to increased distress, and that can reveal itself in many different ways, around social isolation and around their mood. There are a whole range of issues that young people have identified as a result of cyberbullying, which then link to high levels of distress. I think we know that there's a link between high levels of distress and suicide. Whether you can always necessarily draw that direct line is, I think, a question to be asked.[45]

2.37 Dr Buhagier further explained that '[w]e know that there is a link between A and B and between B and C, but to then directly draw a link from A to C is not always as straightforward as we would like.' However, she also noted that '[i]f you're asking me whether reducing or preventing cyberbullying is positive in terms of mental health outcomes and distress, I would say, "Definitely."'[46]

2.38 Professor Campbell was particularly clear when questioning the notion of a direct link between cyberbullying and suicide:

> There has been no causal link shown between any kind of bullying and anybody dying by suicide. There are always mental health issues involved. A bullying incident might be a trigger. It might be a factor or it might not be, but there are always mental health issues. We know that 30 per cent of children have been bullied in the previous 12 months. They have not died by suicide. So you can't say that there's a link. It is mental health.[47]

Cyberbullying targeting adults

Cyberbullying behaviours targeting adults

2.39 Ms Clarke of yourtown acknowledged that cyberbullying extends beyond children:

> Adults are also guilty of cyberbullying. The internet is rampant with adults from many walks of life verbally abusing and bullying others in light of their views, their appearance or some aspect of their life. Indeed, it often feels like the internet is the new Wild West, where social norms are yet to be instilled and where many people aggressively vent their own frustrations.[48]

2.40 The committee heard that cyberbullying of adults is often anonymous trolling where the perpetrator does not personally know the victim. The Media, Entertainment

45 Dr Buhagiar, ReachOut Australia, *Committee Hansard*, 7 March 2018, p. 35.

46 Dr Buhagiar, ReachOut Australia, *Committee Hansard*, 7 March 2018, p. 35.

47 Professor Campbell, AUARA, *Committee Hansard*, 9 February 2018, p. 5.

48 Ms Clarke, yourtown, *Committee Hansard*, 9 February 2018, p. 21.

& Arts Alliance (MEAA) expressed that '[a] great concern is how many cyberbullies hide behind anonymity in order to mount their attacks.'[49]

2.41 The eSafety Commissioner stated that:

> I can tell you from my experience working inside Twitter, I have seen the worst and the worst of determined trolls and what they can do to savage and destroy people's lives. Wily trolls will buy a different SIM card every day for the sole purpose of finding a way to menace the same person. So those people do exist.[50]

2.42 Ms Ginger Gorman, Committee Member of Women in Media, described her research on extreme trolling. She explained that some people troll '…for up to 30 hours a week', and that '…they want to hurt people and they take pleasure in it.' She argued that trolling causes terrible consequences:

> …trolls are wrecking lives. They're causing people, especially women, to harm themselves, to lose their jobs, as Jenna [Price] has mentioned, and to die by suicide. They deliberately wreck a person's reputation so that the person becomes unemployable. It's essentially a type of economic vandalism.[51]

2.43 Ms Van Badham, Media Section Vice President at the MEAA, quoted some extremely violent and vulgar tweets she has received following her public journalistic work. She stated that some of the men who sent these communications to her had enough '…confidence…' to identify themselves with their own names.[52] She also linked trolling to physically violent incidents that she has also experienced:

> …these things are creating a context where violence and harassment is spilling over into real life. Effectively, I have been dehumanised on the internet and represented by these groups of people, sometimes quite deliberately, in a way where they are incited by others towards violence against my person.[53]

Groups that are particularly affected

2.44 Some submitters argued that cyberbullying is a particular problem for those who work in public-facing media roles.[54] Maurice Blackburn Lawyers referred to employment expectations for journalists to '…participate in on-line discussions…' and

---

49 Media, Entertainment & Arts Alliance (MEAA), *Submission 28*, p. 6.

50 Ms Inman Grant, eSafety Commissioner, *Committee Hansard*, 9 February 2018, p. 64.

51 Ms Ginger Gorman, Committee Member, Women in Media, *Committee Hansard*, 9 February 2018, p. 34.

52 Ms Van (Vanessa) Badham, Media Section Vice President, MEAA, *Committee Hansard*, 7 March 2018, p. 12; also see Women in Media, *Submission 26*, pp. 8–11.

53 Ms Badham, MEAA, *Committee Hansard*, 7 March 2018, p. 13.

54 Women in Media, *Submission 26*, p. 5; MEAA, *Submission 28*, p. 3; Maurice Blackburn Lawyers, *Submission 29*, p. 2.

'…express personal opinions…'. It expressed concern that '…these "forced" interactions are exposing media professionals to cyberbullying.'[55]

2.45 The MEAA submitted that '[t]he lived experience of many MEAA members working in the media industry is of being regularly subjected to harassment, abuse and threats on social media…'.[56] It stated that this can occur at home or at work, 24 hours a day, and that:

> …because of the nature of social media platforms and the encouragement they give to others to "engage", others can join in so that the abuse can swell and compound as others join the frenzy.[57]

2.46 Ms Jenna Price, Committee Member at Women in Media, stated that it is not always possible for journalists to block the offending accounts:

> I used to be able to be really good at blocking and deleting, but these people find ways around it. They do private messages, and I can't block those because I'm a journalist. I need to be able to speak to people who are regular and well intentioned and have interesting things to say.[58]

2.47 Ms Badham of the MEAA expressed this problem as '…a workplace safety issue that affects women disproportionately…'.[59] While acknowledging that male journalists also experience cyberbullying, Ms Price stated that '…women journalists receive three times the number of abusive tweets as what men experience.'[60] Ms Badham referred to a public event she attended with a male colleague, after which she '…received 400 rape and death threats', while her male colleague did not receive any.[61]

2.48 Women in Media provided a several reasons as to why a person might cyberbully or troll one of its members:[62]

- they find it amusing;
- they do not like the other person's ideas or ideology;
- another social media user or media personality has initiated the abuse and they are following suit;

---

55 Maurice Blackburn Lawyers, *Submission 29*, p. 2; also see, Ms Badham, MEAA, *Committee Hansard*, 7 March 2018, pp. 13–15.

56 MEAA, *Submission 28*, p. 5.

57 MEAA, *Submission 28*, p. 8.

58 Ms Jenna Price, Committee Member, Women in Media, *Committee Hansard*, 9 February 2018, p. 29.

59 Ms Badham, MEAA, *Committee Hansard*, 7 March 2018, p. 16; also see Women in Media, *Submission 26*, p. 5.

60 Ms Price, Women in Media, *Committee Hansard*, 9 February 2018, p. 29–30.

61 Ms Badham, MEAA, *Committee Hansard*, 7 March 2018, p. 12.

62 Women in Media, *Submission 26*, pp. 7–8.

- they don't consider it to be a big deal or illegal, "it's just words";
- the don't believe there will be any consequences to their actions, or
- they feel they are anonymous.

2.49 In addition to cyberbullying of female journalists, submitters highlighted cyberbullying of women more generally. Victorian Women Lawyers emphasised that:

> Australian women and girls are more likely to be the victims of cyberbullying, with young women particularly vulnerable to many forms of cyberbullying including sexual harassment and stalking.[63]

2.50 The National Council for Single Mothers & their Children stated that '[i]t appears that some of most horrifying abuse and threats are reserved for women who speak out or those deemed to be feminist.'[64]

2.51 The Dr Merrindahl Andrew, Program Manager at the Australian Women Against Violence Alliance (AWAVA), argued that '…cyberbullying is also a manifestation of technology facilitated abuse…', and that:

> …it is important to understand that violence and bullying generally are strongly interlinked with dynamics of gender and sexuality. The normalisation of male violence and restrictive expectations about women and girls are some of the key drivers of violence and bullying generally.[65]

2.52 Ms Gorman of Women in Media argued that cyberbullying and trolling '…disproportionately affects women, especially black women, people of colour and transwomen.'[66] Mr Andrew Jakubowicz argued that some cyberbullying is linked with racism.[67] Additionally, AWAVA highlighted a recent survey which '…concluded that people with disability, Aboriginal and Torres Strait Islander people and people who identify as LGBTIQ are particularly vulnerable to technology-facilitated abuse.'[68]

A nationally consistent definition of 'cyberbullying'

2.53 Several submitters supported the development of a clear definition of cyberbullying.[69] The Law Council of Australia submitted that '[t]he definition of "cyberbullying" is not universal and is open to debate.'[70] It emphasised:

---

63 Victorian Women Lawyers, *Submission 5*, p. 3.

64 National Council of Single Mothers & their Children, *Submission 7*, p. 1.

65 Dr Merrindahl Andrew, Program Manager at the Australian Women Against Violence Alliance, *Committee Hansard*, 9 February 2018, p. 32.

66 Ms Gorman, Women in Media, *Proof Committee Hansard*, 9 February 2018, p. 34.

67 Mr Andrew Jakubowicz, *Submission 30*, pp. 1–3.

68 Australian Women Against Violence Alliance, *Submission 14*, p. 2.

69 See, for example, yourtown, *Submission 6*, p. 4; MEAA, *Submission 28*, p. 7; Professor Campbell, AUARA, *Committee Hansard*, 9 February 2018, p. 1; Ms Mitchell, National Children's Commissioner, Australian Human Rights Commission, *Committee Hansard*, 9 February 2018, p. 53.

70 Law Council of Australia, *Submission 15*, p. 7.

> …the need for common understanding of conduct which constitutes cyberbullying, and the perpetrators involved, as a necessary basis for assessing possible law reform options in this area.[71]

2.54 Mr Blackman of the Alannah and Madeline Foundations stated that '[i]n many respects, cyberbullying is still an adult-conceived term.'[72] His colleague, Ms Podesta, advocated '…bring[ing] together a range of organisations to try to get some agreed, common definition' of cyberbullying:

> …we don't believe that we have reached an appropriate definition of cyberbullying, which is why we would issue caution about going down a legislation path now. There isn't an agreed community understanding of what this means. As I think all of us have said today, the issue of 'readily understandable' is critical in this. You can't change behaviours if people don't know what you're talking about.[73]

2.55 Mr Dalgleish of yourtown stated that '[t]he law sets behavioural standards in our community, so we do need some template about what it is we're talking about.'[74] He also indicated some possible features of a cyberbullying definition when discussing the difference between teasing and bullying:

> I will kick off by saying that the difference is two things. It's ongoing, so it's not a one-off; it's an ongoing pattern of behaviour and intent—intent to humiliate or to hurt. Teasing might be in a particular context; it might be a one-off. But, when you see a pattern emerging, when it's an ongoing behaviour with that intent, then, to me, that's when it passes the line to bullying and cyberbullying.[75]

2.56 Ms Gorman of Women in Media referred to '…a very good definition that comes out of the cyberbullying centre in the US, which is to do with repetitive attacks with the intent to cause harm using an electronic device, so it's very specific.'[76] Some submitters also noted that bullying is already defined in a workplace context.[77]

2.57 The eSafety Commissioner stated that '[t]here is a definition of serious cyberbullying in the [*Enhancing Online Safety Act 2015*].'[78] The meaning of '…cyberbullying material targeting an Australian child…' is set out in section 5 of this

---

71 Law Council of Australia, *Submission 15*, p. 5.

72 Mr Blackman, Alannah & Madeline Foundation, *Committee Hansard*, 9 February 2018, p. 23.

73 Ms Podesta, Alannah & Madeline Foundation, *Committee Hansard*, 9 February 2018, p. 26.

74 Mr Dalgleish, yourtown, *Committee Hansard*, 9 February 2018, p. 24; also see Alannah & Madeline Foundation, *Submission 10*, p. 6.

75 Mr Dalgleish, yourtown, *Committee Hansard*, 9 February 2018, p. 26.

76 Ms Gorman, Women in Media, *Committee Hansard*, 9 February 2018, p. 31.

77 Alannah & Madeline Foundation, *Submission 10*, pp. 2–3; Maurice Blackburn Lawyers, *Submission 29*, p. 2.

78 Ms Inman Grant, eSafety Commissioner, *Committee Hansard*, 9 February 2018, p. 62.

Act. Under subsection 5(1), material meets the definition if it satisfies the following conditions:

> (a) the material is provided on a social media service or relevant electronic service;
>
> (b) an ordinary reasonable person would conclude that:
>
> (i) it is likely that the material was intended to have an effect on a particular Australian child; and
>
> (ii) the material would be likely to have the effect on the Australian child of seriously threatening, seriously intimidating, seriously harassing or seriously humiliating the Australian child;
>
> (c) such other conditions (if any) as are set out in the legislative rules

2.58 The eSafety Office explained that:

> [w]hether the 'serious' threshold is met under the Act will depend on the facts and circumstances of every individual complaint. The Explanatory Memorandum to the Act makes clear that material must be more than merely 'offensive or insulting' to be considered cyberbullying material. The age and characteristics of the child will also be relevant, as will the sensitivity of the material and the number of times it has been viewed or shared.[79]

2.59 The committee is aware that the interim report of the Australian Parliamentary Joint Select Committee on Cyber-Safety, tabled in June 2011, recommended:

> [t]hat the Minister for Broadband, Communications and the Digital Economy invite the Consultative Working Group on Cybersafety, in consultation with the Youth Advisory Group, to develop an agreed definition of cyber-bullying to be used by all Australian Government departments and agencies, and encourage its use nationally.[80]

2.60 The committee also notes the Australian Government's response to that inquiry, dated December 2011, which accepted the above recommendation. It stated:

> The Safe and Supportive School Communities (SSSC) is a Working Group of the Australian Education, Early Childhood Development & Youth Senior Officials Committee (AEEYSOC). The Working Group includes nominated representatives of all Australian education jurisdictions - all state, territory and federal education departments as well as national Catholic and independent schooling representatives.
>
> The SSSC working group has developed the following definition of cyberbullying:
>
> > "Bullying is repeated verbal, physical, social or psychological behaviour that is harmful and involves the misuse of power by an

79 eSafety Office, *Submission 13*, p. 4.

80 Joint Select Committee on Cyber-Safety, *High-Wire Act: Cyber-Safety and the Young*, June 2011, p. xxvi.

> individual or group towards one or more persons. Cyberbullying refers to bullying through information and communication technologies."[81]

2.61 The government response stated that various groups would be consulted on this definition, and that '[t]he definition will be discussed and agreed by state and territory governments through AEEYSOC.' The agreed definition would then be promoted nationally.[82]

2.62 The committee was not able to identify the current status of this definition. The committee makes a recommendation about the definition of cyberbullying in Chapter 5.

81 Australian Government, *Government Statement of Response: Joint Select Committee on Cyber-Safety Interim Report – High-Wire Act: Cyber-safety and the Young*, December 2011, pp. 5–6.

82 Australian Government, *Government Statement of Response: Joint Select Committee on Cyber-Safety Interim Report – High-Wire Act: Cyber-safety and the Young*, December 2011, p. 6.

Chapter 3

Criminal offences for cyberbullying

3.1 This chapter will outline the evidence the committee heard about:

- the role of criminal offences with regard to cyberbullying;
- the current criminal offences that could apply to cyberbullying; and
- the adequacy of these offences.

The role of criminal offences

3.2 The Mental Health Commissions of Australia argued that '…the problem of cyberbullying is not fundamentally a legal problem, but a social one.'[1] Many submitters made a similar point.[2]

3.3 Accordingly, a number of submitters emphasised the importance of preventative social measures to address cyberbullying.[3] As the Office of the eSafety Commissioner (eSafety Office) argued:

> …addressing cyberbullying behaviour through criminal sanctions is only effective after the behaviour has been perpetrated. It's arguable that in most instances this will be too late in the process as the harm will have been done to a number of parties. The Commissioner considers that the most effective measure to address cyberbullying is prevention, in the first instance, followed by early intervention through reporting, education and harm minimisation – before the escalation of conduct reaches a criminal level.[4]

3.4 The Tasmanian Government submitted that '[n]ot all cyberbullying conduct should attract criminal liability…', but also acknowledged that '[s]ome forms of cyberbullying justify a criminal justice response owing to the very serious harm that bullying can cause a victim.'[5]

---

1 Mental Health Commissions of Australia, *Submission 9*, p. 5.

2 See, for example, Australian Universities' Anti-bullying Alliance (AUARA), *Submission 1*, p. 5; Office of the eSafety Commissioner (eSafety Office), *Submission 13*, p. 12; Ms Laura Clarke, Advocacy and Policy Lead, yourtown, *Committee Hansard*, 9 February 2018, p. 21; Ms Megan Mitchell, National Children's Commissioner, Australian Human Rights Commission (AHRC), *Committee Hansard*, 9 February 2018, p. 55.

3 See, for example, yourtown, *Submission 6*, p. 2; Ms Lesley Podesta, Chief Executive Officer, Alannah & Madeline Foundation, *Committee Hansard*, 9 February 2018, p. 28; Dr Merrindahl Andrew, Program Manager, Australian Women Against Violence Alliance (AWAVA), *Committee Hansard*, 9 February 2018, p. 32; Mrs Liza Davis, Director of Strategic Communications and Government Relations, ReachOut Australia, *Committee Hansard*, 7 March 2018, p. 31.

4 eSafety Office, *Submission 13*, p. 2.

5 Tasmanian Government, *Submission 19*, p. 2 and p. 7.

3.5 A number of submitters also argued, particularly with respect to children, that criminal offences should only be applied in the most serious cyberbullying cases.[6] Professor Phillip Slee, Member of the Australian Universities' Anti-bullying Research Alliance (AUARA), argued that:

> …the criminalisation of young people really does lead to a lot of unfortunate sequela. Criminalisation leads to school disengagement, and the evidence is that it leads to a reduction in academic performance. It ultimately leads to the juvenile justice system, and that's where we would not think there is a role.[7]

3.6 The Law Council of Australia (Law Council) supported '…effective minimum standards for the sentencing of young offenders who may be perpetrators of cyberbullying.'[8] The Australian Human Rights Commission (AHRC) argued that, when considering criminal sanctions, '…different standards should apply for addressing behaviour of children than for adults.'[9] Similarly, yourtown supported '…discretion and preferably a case-by-case approach to legislation involving young people.'[10] It advanced that:

> …bullying arises as children and young people explore and push social and relational boundaries, and undergo key transitions through school and puberty. During this process, they will make mistakes, misjudge or not fully consider the consequences of their actions, and an excessively punitive response from our legal system would mean these impulsive mistakes and lack of judgement could result in long-lasting impacts on their future lives.[11]

3.7 In addition, Ms Lesley Podesta, Chief Executive Officer at the Alannah & Madeline Foundation, stated that criminal offences must be considered carefully because children who perpetrate cyberbullying may also be victims of it.[12]

3.8 The Alannah & Madeline Foundation also argued that criminal offences can be used to send a message to society:

---

6 See, for example, Facebook, *Submission 4*, p. 8; yourtown, *Submission 6*, p. 11; Ms Vanessa D'Souza, Acting Director, Policy, Analysis and Reporting, National Mental Health Commission, *Committee Hansard*, 9 February 2018, p. 54; Ms Mitchell, National Children's Commissioner, AHRC, *Committee Hansard*, 9 February 2018, pp. 54–55; Ms Julie Inman Grant, eSafety Commissioner, Office of the eSafety Commissioner, *Committee Hansard*, 9 February 2018, p. 62; Ms Anna Harmer, First Assistant Secretary, Security and Criminal Law Division, Attorney-General's Department, *Committee Hansard*, 7 March 2018, p. 49.

7 Professor Phillip Slee, Member, AUARA, *Committee Hansard*, 9 February 2018, p. 3.

8 Law Council of Australia (Law Council), *Submission 15*, p. 14.

9 AHRC, *Submission 16*, p. 1; also see Alannah & Madeline Foundation, *Submission 10*, p. 6.

10 yourtown, *Submission 6*, p. 12.

11 yourtown, *Submission 6*, p. 11; also see Ms Mitchell, National Children's Commissioner, AHRC, *Committee Hansard*, 9 February 2018, pp. 54–55.

12 Ms Podesta, Alannah & Madeline Foundation, *Committee Hansard*, 9 February 2018, p. 24.

> The law itself is an educational tool. Laws are in place to act as a deterrent and impact upon behaviours – to teach people that there are acceptable and unacceptable ways to behave. This is further reason to have a nationalised standard legal definition of cyberbullying and to leverage the law to educate our community that such behaviour is unacceptable.[13]

Existing criminal offences in the *Criminal Code Act 1995* (Commonwealth)

3.9 The Attorney-General's Department submitted that '[t]he Criminal Code does not define "cyberbullying".'[14] However, there are a number of offences in the Criminal Code that could be relevant to cyberbullying, including:[15]

- section 474.14 (using a telecommunications network with intention to commit a serious offence);
- section 474.15 (using a carriage service to make a threat);
- section 474.16 (using a carriage service for a hoax threat);
- section 474.17 (using a carriage service to menace, harass or cause offence); and
- section 474.29A (using a carriage service for suicide related material).

3.10 Section 474.17 is the most notable of these offences. It carries a maximum penalty of three years' imprisonment. Subsection 474.17(1) states that:

> (1) A person commits and offence if:
>
> (a) the person uses a carriage service; and
>
> (b) the person does so in a way (whether by the method of use or the content of a communication, or both) that reasonable persons would regard as being, in all the circumstances, menacing, harassing or offensive.

3.11 The Attorney-General's Department explained that '…the prosecution would not have to prove that the accused intended to menace, harass or cause offence.'[16] However, the offender must '…have been reckless as to whether they were using a carriage service in a way that the "reasonable person" would regard, in all the circumstances, as menacing, harassing or offensive.'[17]

3.12 Regarding the meaning of 'menace, harass, or cause offence', the Attorney-General's Department explained:

---

13 Alannah & Madeline Foundation, *Submission 10*, p. 6; also see, for example, Professor Marilyn Campbell, Founding Member, AUARA, *Committee Hansard*, 9 February 2018, p. 5; Mr John Dalgleish, Head of Strategy and Research, yourtown, *Committee Hansard*, 9 February 2018, p. 24.

14 Attorney-General's Department, *Submission 20*, p. 5.

15 Law Council, *Submission 15*, p. 11.

16 Attorney-General's Department, *Submission 20*, p. 5.

17 Attorney-General's Department, *Submission 20*, p. 5.

> Section 474.17 does not further define what constitutes menacing, harassing or offensive conduct. This enables community standards and common sense to be imported into a decision on whether the conduct is in fact menacing, harassing or offensive.
>
> However, section 474.17 was constructed to ensure the use of a carriage service by a person can be menacing, harassing or offensive to the reasonable person because of the *way* the carriage service has been used or the *content* of the communication, or both.[18]

3.13 The Attorney-General's Department further explained that when determining whether conduct is offensive, the matters to consider include:

> …standards of morality, decency and propriety generally accepted by reasonable adults, the literary, artistic or educational merit (if any) of the material, and the general character of the material, including whether it is of a medical, legal or scientific character.[19]

3.14 The Law Council referred to High Court precedent (*Monis v R; Droudis v R (2013) 249 CLR 92*) and explained that Crennan, Kiefel and Bell JJ:

> …held that the words "menacing" and "harassing" imply serious potential effect upon an addressee, one which cause an apprehension, if not a fear, for that person's safety. For consistency, to be "offensive" a communication must be likely to have a serious effect upon the emotional well-being of an addressee.[20]

3.15 According to data from the Commonwealth Director of Public Prosecutions, there have been 927 charges against 458 defendants found proven under section 474.17 since it was introduced in 2004.[21] The Attorney-General's Department stated that it is not possible to specify how many of these cases relate to cyberbullying, but '…numerous instances…' of cyberbullying have been prosecuted under section 474.17. In addition, these figures do not include prosecutions conducted by state or territory authorities which are also able to prosecute Commonwealth Criminal Code offences.[22] However, none of the charges or prosecutions that the committee is aware of appear to relate to cyberbullying between school aged children. This demonstrates that while the ability to prosecute exists in theory, in practice it is not a deterrent to school aged children which amplifies the need to have other deterrent approaches to cyberbullying when children are involved.

---

18 Attorney-General's Department, *Submission 20*, p. 6.

19 Attorney-General's Department, *Submission 20*, p. 6; also see Victorian Women Lawyers, *Submission 5*, p. 4;Western Australia Police Force, *Submission 11*, p. 3.

20 Law Council, answers to questions on notice, 9 February 2018 (received 5 March 2018), pp. 2–3.

21 Attorney-General's Department, *Submission 20*, p. 7.

22 Ms Harmer, Attorney-General's Department, *Committee Hansard*, 7 March 2018, pp. 48–49.

The adequacy of existing criminal offences

3.16 Some submitters and witnesses stated that legislative reform should be considered. The Media, Entertainment & Arts Alliance (MEAA) argued that many of the current state regimes are 'deficient', and also that:

> …section 474.17 [of the Commonwealth Criminal Code] has not kept pace with the rise of offences it seeks to curtail and punish. The tools of cyberbullying are readily available, easily used, allow for anonymous attacks and enable viral assaults.[23]

3.17 Victorian Women Lawyers argued that '…there is currently a gap in the law in relation to the area of cyberbullying and it should be addressed in order to protect women.'[24] For instance, it argued that due to current judicial interpretations:

> …the application of [section 474.17] is limited in providing justice in that it is not enough that the conduct simply hurt or wound the feelings of the recipient in the mind of a reasonable person.[25]

3.18 Women in Media also submitted that there are '…gaps which are being identified, including new offences, emerging trends, and cybercrime dependent crimes which may not be covered adequately by Section 474.17.'[26] It recommended that '…funding be allocated to research on new offences, emerging trends and crimes which are dependent or enabled by the use of social media and telecommunications services.'[27]

3.19 The Carly Ryan Foundation suggested consideration of:

> …a straight up bullying charge, which comes with certain criteria that mimics stalking legislation and can issue a no contact order at court upon conviction under the bullying legislation that there is no contact for a reasonable time.[28]

3.20 The committee heard a number of other options for legislative reform, including the following:

- Maurice Blackburn Lawyers highlighted that journalists and others may experience cyberbullying at work, and submitted that:

  > …changes to the regulatory environment in relation to cyberbullying must include enforceable sanctions against employers who fail in their duty to provide a safe workplace for their employees.[29]

---

23 Media, Entertainment & Arts Alliance (MEAA), *Submission 28*, p. 7 and p. 8.

24 Victorian Women Lawyers, *Submission 5*, p. 3.

25 Victorian Women Lawyers, *Submission 5*, p. 4.

26 Women in Media, *Submission 26*, p. 12; also see UNSW Law Society Inc., *Submission 32*, p. 11.

27 Women in Media, *Submission 26*, p. 12.

28 Carly Ryan Foundation, *Submission 23*, p. 3.

29 Maurice Blackburn Lawyers, *Submission 29*, p. 3.

- The Carly Ryan Foundation suggested '…an intervention order scheme…' which '…would be mirrored on domestic violence orders which are issued by police or a court upon application by a victim…'. Further, there would be '…criminal penalties imposed where an order is contravened.'[30]
- Consider reforms to enable authorities to suspend internet access, or some forms of internet access, from those who repeatedly perpetrate serious cyberbullying.[31]

3.21 However, some submitters, including the Law Council and AUARA, argued that existing offences in the Criminal Code and in state and territory criminal laws are adequate to deal with serious cyberbullying.[32]

3.22 More specifically, both these groups also argued that that the introduction of a law that criminalises cyberbullying explicitly is not necessary.[33] AUARA referred to '…evidence from America that shows that criminalisation of school bullying has not resulted in a decrease in the behaviour.'[34] AUARA also submitted that a specific cyberbullying law '…would likely not deter young people and could possibly do more harm than good.'[35]

3.23 The Attorney-General's Department stated that '…more specific offences may not necessarily make cyberbullying conduct easier to prosecute. Indeed, the converse may be true.'[36] It stated that the offence under section 474.17 '…is broadly framed and applies to a range of conduct…', and explained:

> This approach is consistent with Commonwealth criminal law policy, which prefers offences of general application over numerous slightly different offences of similar effect. General offences criminalising classes of conduct avoids the technical distinctions, loopholes and additional prosecution difficulty or appearance of incoherence that can be associated with multiple more specific offences. The existing offences in the Criminal Code are also technologically neutral, focusing on the harmful conduct of the perpetrator rather than any specific communications service or platform. This makes them applicable to the wide range of communications services and public platforms now in use as well as resistance to frequent rapid changes in communications technology.[37]

---

30 Carly Ryan Foundation, answers to questions on notice, 7 March 2018 (received 14 March 2018).

31 Carly Ryan Foundation, *Submission 23*, p. 2; The Hon. Shelley Hancock MP, Speaker of the NSW Legislative Assembly, *Submission 33*, p. 4; Ms Van (Vanessa) Badham, Media Section Vice President, Victorian Branch, MEAA, *Committee Hansard*, 7 March 2018, pp. 16–17.

32 Law Council, *Submission 15*, p. 5; AUARA, *Submission 1*, p. 3.

33 Law Council, *Submission 15*, p. 11; AUARA, *Submission 1*, p. 3.

34 AUARA, *Submission 1*, p. 4.

35 AUARA, *Submission 1*, p. 6.

36 Ms Harmer, Attorney-General's Department, *Committee Hansard*, 7 March 2018, p. 49.

37 Ms Harmer, Attorney-General's Department, *Committee Hansard*, 7 March 2018, p. 48.

3.24 The New South Wales Police Force explained that although there is no explicit cyberbullying law in New South Wales:

> …we can criminalise cyberbullying, stalking or harassment with other laws. For instance, under the Crimes Act we might look at domestic or personal violence or at stalking. Then we can also use the Criminal Code Act to look at the offences using a carriage service, so using a phone or a computer to menace, harass or cause offence.[38]

3.25 The Western Australia Police Force also submitted that existing laws are generally adequate, and argued that '…any move to widen the scope would significantly increase crime reports, exceed existing police resources and draw police into a range of non-core activities that ought not attract criminal culpability.'[39]

3.26 Additionally, the Digital Industry Group Incorporated (DIGI) cautioned against premature reform. It submitted that '[v]ictims of cyberbullying are already able to take action under various laws and schemes in addition to the *Criminal Code Act 1995*', including under the *Telecommunications (Interception and Access) Act 1979*, the *Privacy Act 1988*, the *Defamation Act 2005*, and state and territory defamation acts. DIGI argued:

> In order to get a clearer picture of the problem and the number of people resorting to legal processes, it's important to know the exact number of cases brought forward under these existing laws. For this reason, DIGI contends that existing legislative frameworks are highly relevant to this consultation and should be reviewed before any new additional laws are considered.[40]

General considerations in any legislative reform

3.27 Professor Campbell of AUARA argued that, while existing laws are sufficient to address serious cases of cyberbullying, '…there needs to be a harmonisation of these laws nationally, because we have different laws in different states with different definitions.'[41] Similarly, yourtown recommended that:

> …federal and state legislation be simplified and harmonised and that a nationally consistent legislative approach to, as well as a definition of, cyberbullying be developed. This clarity would undoubtedly support more efficient and effective legal redress of serious cyberbullying crimes by the police and legal agencies. It's also likely to help better position relevant legislation as a deterrent to cyberbullying through supporting an increased

38 Detective Chief Inspector Carlene Mahoney, Strategic Coordinator, Youth and Crime Prevention Command, New South Wales Police Force, *Committee Hansard*, 7 March 2018, p. 37.

39 Western Australia Police Force, *Submission 11*, p. 3.

40 Digital Industry Group Incorporated, *Submission 17*, p. 9.

41 Professor Campbell, AUARA, *Committee Hansard*, 9 February 2018, p.1.

> understanding of the law by children, young people and the wider community.[42]

3.28 The Law Council argued that human rights principles and rule of law principles should be taken into account when considering any legislative measures to address cyberbullying. It highlighted relevant human rights and advanced that:

> …any Australian Government response to cyberbullying should explicitly address these competing interests. It should then seek to balance these interests in a manner which ensures that any limitations placed on individuals' rights are necessary, reasonable and proportionate.[43]

3.29 In addition, the Law Council advanced '…key rule of law principles…' including that '…the law must be both readily known and available, and certain and clear.'[44]

3.30 The Australian Women Against Violence Alliance argued that '…people with disability, Aboriginal and Torres Strait Islander people and people who identify as LGBTIQ are particularly vulnerable to technology-facilitated abuse.'[45] It recommended that:

> …in pursuing law reform, jurisdictions consider how criminal penalties can work together with antidiscrimination laws to treat cyberbullying on the grounds of sexuality, culture, race, gender, disability and religion as particularly serious offences.[46]

3.31 Additionally, the Queensland Mental Health Commission stated that:

> …there are some circumstances where a person's mental illness could directly contribute to them engaging in behaviour that is deemed online harassment or bullying. For example, if they are experiencing acute symptoms of mania, delusions, impulsivity or emotional dysregulation.[47]

3.32 The Mental Health Commissions of Australia submitted that '[l]aws regarding cyberbullying should offer sufficient safeguards to ensure people engaging in cyberbullying as a direct result of their mental illness receive an appropriate response.'[48]

---

42 Ms Clarke, yourtown, *Committee Hansard*, 9 February 2018, p. 21; also see Victorian Women Lawyers, *Submission 5*, p. 3; AWAVA, *Submission 14*, p. 2.

43 Law Council, *Submission 15*, p. 9.

44 Law Council, *Submission 15*, p. 9.

45 AWAVA, *Submission 14*, p. 2.

46 AWAVA, *Submission 14*, p. 3; also see Mr Andrew Jakubowicz, *Submission 30*, p. 3.

47 Queensland Mental Health Commission, answers to questions taken on notice by the National Mental Health Commission, 9 February 2018 (received 6 March 2018).

48 Mental Health Commissions of Australia, *Submission 9*, p. 6.

An offence against the broadcasting of crimes

3.33 Victorian Women Lawyers argued that '…existing laws applicable to broadcasting crimes on social media are many and varied nationwide.'[49] It advocated:

> …establishing a law that specifically addresses this issue, similar to what has been enacted in South Australia under the Summary Offences Act, which creates an offence to criminalise those who film and distribute footage of humiliating and degrading acts without the consent of victims.[50]

3.34 The Northern Territory Police Force (NT Police) suggested that '[s]tate based legislation targeting posting of unlawful behaviour…' may be beneficial. It submitted:

> There have been instances in the Northern Territory (NT) where offences (most notably assaults) have been broadcast from social media platforms.
>
> Requests to remove these posts from social media have been declined by Facebook on the grounds that Facebook did not believe the material published on the page breached community standards. No further recourse is available to have these decisions reconsidered. This remains an issue for the NT.[51]

3.35 The Tasmanian Government also submitted that '…a range of enforcement mechanisms and offences…' may be beneficial, but noted that the broadcasting of offences '…is not a circumstance with which any particular issues have currently been identified…'.[52] Similarly, the eSafety Office stated that '[t]o date, the eSafety Commissioner has not received a complaint dealing with the "broadcasting" of assaults or other crimes via social media platforms.'[53]

3.36 The Attorney-General's Department submitted that existing legislation may already be applied to the broadcasting of offences, including offences relating to child exploitation material and section 474.14 of the Criminal Code (using a telecommunications network with intention to commit a serious offence).[54]

3.37 The Law Council '…appreciates the interest in enacting provisions to target the use of a carriage service to broadcast assaults or other criminal acts', but does not support a new offence for the broadcasting of offences.[55] It argued that '…many cases where crimes or assaults are broadcast would easily fall within the definition of

---

49 Victorian Women Lawyers, *Submission 5*, p. 3–4.

50 Mss Alex Dworjanyn, Law Reform Committee Co-Chair, Victorian Women Lawyers, *Committee Hansard*, 9 February 2018, p. 14; also see South Australian Government, *Submission 21*, pp. 2–5.

51 Northern Territory Police Force, *Submission 22*, p. 2.

52 Tasmanian Government, *Submission 19*, p. 4.

53 eSafety Office, *Submission 13*, p. 3.

54 Attorney-General's Department, *Submission 20*, pp. 10–11.

55 Law Council, *Submission 15*, pp. 11–12.

section 474.17', and also that a new offence may cause confusion about its overlap with the existing offence.[56]

3.38 The Law Council further argued that if such a law were introduced, then '…the consent of the Attorney-General should be required before a person under the age of 18 could be charged with an offence.'[57] Mr Arthur Moses SC of the Law Council stated that this would be '…in order to ensure that only the most serious examples of alleged offending by children would be prosecuted.'[58]

3.39 DIGI and Facebook also opposed a new offence for the broadcasting of offences. DIGI noted that users' live streamed content sometimes provides '…invaluable evidence…' during court proceedings.[59] Facebook posited that '…it may be too difficult to fashion a criminal law that permits positive uses of [Facebook] Live and only criminalises inappropriate uses of Live.' It further argued that its Community Standards apply to Facebook Live, and that '[p]latforms such as ours are already committed to working with law enforcement in relation to these types of issues.'[60]

Implementation of existing criminal offences by police

3.40 The committee heard that, in some instances, police may not be fully aware of existing criminal offences.[61] As the Law Council submitted:

> Research shows that police often refuse to lodge complaints from disgruntled victims of cyberbullying because of their lack of knowledge of the various laws applicable to incidents of cyberbullying.
>
> There may be value, therefore, for increased education and awareness of the possible consequences of cyberbullying, for law enforcement, prosecutors and the judiciary.[62]

3.41 Similarly, the MEAA referred to a June 2014 report of the Australian Law Reform Commission. It quoted the report as stating:

> In consultations the [Australian Law Reform Commission] heard concerns raised that state and territory police may be unwilling or unable to enforce criminal offences due to a lack of training and expertise in Commonwealth

56 Law Council, *Submission 15*, pp. 11–12.

57 Law Council, *Submission 15*, p. 5.

58 Mr Arthur Moses SC, President-elect, Law Council, *Committee Hansard*, 9 February 2018, p. 8.

59 Digital Industry Group Incorporated, *Submission 17.1*, p. 1.

60 Facebook, *Submission 4*, pp. 8–9.

61 See, for example, AWAVA, *Submission 14*, pp. 3–4; Digital Industry Group Incorporated, *Submission 17.1*, p. 1; UNSW Law Society Inc., *Submission 32*, p. 16; Miss Hayley Chester, Law Reform Committee Co-Chair, Victorian Women Lawyers, *Committee Hansard*, 9 February 2018, p. 14; Mr Adam Portelli, Director, Victorian Branch, MEAA, *Committee Hansard*, 7 March 2018, p. 10.

62 Law Council, *Submission 15*, p. 18.

> procedure which often differs significantly from state and territory police procedures.[63]

3.42 Ms Ginger Gorman of Women in Media likened the current situation to '…where we were with domestic violence 30 years ago. Nobody thought it was serious; everybody thought it was someone else's problem.' She stated that she called the police after her children received threats, and the police said '…"[s]tay off the internet, Love."'[64]

3.43 In addition, the National Council of Single Mothers and their Children (NCSMC) referred to difficulties they experienced with police investigating cyberbullying complaints. In one instance, Ms Terese Edwards, Chief Executive Officer, reported to the Australian Cybercrime Online Reporting Network (ACORN) a series of threats that she and other women had received. The ACORN then referred the matters to relevant state police forces, but because the women lived in different states, the respective police forces treated different parts of the matter in isolation, rather than as one whole. The threats caused great distress to the women involved.[65] The committee notes that, from a policing perspective, this is an inefficient approach to a serious problem.

3.44 In another case, Ms Jenna Oakley of the NCSMC told the committee about online abuse she received from an ex-partner. She stated that Victoria Police told her it could not take action without the alleged perpetrator's IP address, which it could not access due to Victorian privacy law.[66]

3.45 Further, the New South Wales Police Force (NSW Police) stated that when the cyberbully acts anonymously, it can be much more difficult for the police to identify the perpetrator and investigate the matter.[67]

3.46 yourtown noted that police must operate with limited resources:

> Today, we know that stretched police and legal agencies are only able to act on the more serious cases of cyberbullying. To introduce new or strengthen

63 MEAA, *Submission 28*, pp. 4–5.

64 Ms Ginger Gorman, Committee Member, Women in Media, *Committee Hansard*, 9 February 2018, p. 35.

65 National Council of Single Mothers and their Children, Submission 7, pp. 2–3; Ms Terese Edwards, Chief Executive Officer, National Council of Single Mothers and their Children, *Committee Hansard*, 7 March 2018, pp. 26–27.

66 Ms Jenna Oakley, Member, National Council of Single Mothers and their Children, *Committee Hansard*, 7 March 2018, pp. 23–24; It appears that this may not accord with the Attorney-General's Department's statement that state police forces can access IP addresses for criminal matters (see paragraph 3.64).

67 Detective Chief Inspector Carlene Mahoney, Strategic Coordinator, Youth and Crime Prevention Command, New South Wales Police Force, *Committee Hansard*, 7 March 2018, p. 39 and p. 42.

> existing offences would require the cooperation and action of already over committed legal and enforcement agencies.[68]

3.47 The Australian Federal Police (AFP) submitted that '[u]nder current arrangements, State and Territory police have primary carriage for investigating cyberbullying matters.'[69] The AFP further explained that this is '…by agreement under the protocol that was led through an [Australia New Zealand Policing Advisory Agency] forum to set the framework for cybercrime investigations…'.[70]

3.48 The NT Police acknowledged that Commonwealth offences such as section 474.17 are available and '…can be used to fill in gaps in NT legislation', but also stated that:

> [t]he complexities and nuances in using different legislation discourages police members from using this option.
>
> Specific NT legislation to address this activity is preferable as it would better enable the NT Police Force to investigate and prosecute cyberbullying.[71]

3.49 Similarly, the Tasmanian Government submitted that 'Tasmania Police rarely use the Commonwealth Criminal Code offence…under section 474.17.' It explained:

> Investigatory regimes and police powers are significantly different under State and Commonwealth legislation. This includes search warrants, collection of forensic evidence, interview procedures, arrest powers and investigative detention. The majority of state police have no experience with Commonwealth procedures. The Tasmanian Government notes that it is preferable that offending conduct be covered by State-based offences where possible if there is an expectation that the offences will be enforced by state police.[72]

3.50 However, NSW Police confirmed that it has laid charges under section 474.17 of the Commonwealth Criminal Code.[73] The Western Australia Police Force noted that it has:

> …consolidated the management of all Cybercrime matters, which includes, covert online operations and cybercrime investigation and the management of the Australian Online Reporting Network (ACORN) in a single business area…[74]

---

68 yourtown, *Submission 6*, p. 11.

69 Australian Federal Police, *Submission 18*, p. 2.

70 Acting Commander Joanne Lee Cameron, Acting Manager Victim Based Crime, Australian Federal Police, *Committee Hansard*, 7 March 2018, p. 54.

71 Northern Territory Police Force, *Submission 22*, p. 3.

72 Tasmanian Government, *Submission 19*, p. 4.

73 Detective Chief Inspector Mahoney, New South Wales Police Force, *Committee Hansard*, 7 March 2018, pp. 37–38.

74 Western Australia Police Force, *Submission 11*, p. 2.

Awareness of existing criminal offences among the public

3.51 Some submitters suggested that the public is often unaware of existing criminal laws, and therefore the effectiveness of those laws is limited.[75] Miss Hayley Chester, Law Reform Committee Co-Chair at Victorian Women Lawyers, argued that:

> …if our law enforcement are not aware of this law, then it's highly unlikely that a lot of members of the community are going to be aware of the law—having that law there has the impact, obviously, of limited deterrence. So I think there's a really strong need for education for not only law enforcement but also the community in general that, yes, this behaviour is a crime and it can be prosecuted.[76]

3.52 Similarly, Ms Megan Mitchell, National Children's Commissioner at the AHRC, argued that:

> …regardless of whether a law changed, we still need to educate the community and children about it. And I don't believe that is the case currently. I think that there's a problem at the moment in the cyberworld because people don't think laws apply in that space when they clearly do. We think the main issue is: people don't understand the law; they don't know laws exist and, as a message to the community, which laws are important to make.[77]

3.53 However, in its submission, the AHRC also referred to research that '…supports the view that public education and awareness raising programs are likely to be more effective influencers of children's behaviour than additional legal sanctions.'[78]

3.54 The eSafety Commissioner expressed uncertainty about how effective criminal laws may be in deterring young people from cyberbullying:

> **Senator PATRICK:** You were very clear that the best medicine in this instance is to avoid it happening altogether. Surely—and I'm being a bit adversarial here, noting your position—strong laws assist with prevention
>
> **Ms Inman Grant:** I don't know. Maybe we should sit down and talk to a 13- or 14-year-old and see whether a criminal law would serve as a real deterrent to them sending that menacing tweet or post. Young people that age may not understand the implications of the law. They probably wouldn't be able to read and interpret it. You know what? I don't know. I think there probably is a role for criminal laws in this space for the most egregious offenders.[79]

---

75 See, for example, AHRC, *Submission 16*, p. 3; MEAA, *Submission 20*, p. 5 and p. 8.

76 Miss Chester, Victorian Women Lawyers, *Committee Hansard*, 9 February 2018, p. 15.

77 Ms Mitchell, National Children's Commissioner, AHRC, *Committee Hansard*, 9 February 2018, p. 55; also see, for example, Ms Sonya Ryan, Chief Executive Officer and Founder, Carly Ryan Foundation, *Committee Hansard*, 7 March 2018, p. 21.

78 AHRC, *Submission 16*, p. 3.

79 Ms Inman Grant, eSafety Commissioner, *Committee Hansard*, 9 February 2018, p. 64.

3.55 Maurice Blackburn stated that '[c]riminalisation alone will not be the most effective inhibitor of [cyberbullying] behaviours. That section 474.17 has been in existence for more than a decade, its effectiveness as a deterrent is obviously questionable.'[80] AUARA made a clear challenge to any deterrent effect:

> It may be thought that having a specific law against bullying and the fear of punishment may also serve as a deterrent effect. However, it would be naïve to think that simply having a law will curtail the behaviour. After all, there are longstanding and well publicised laws against speeding, but this has not stopped many drivers from speeding. Similarly criminal sanctions against drug use and underage sex do not deter young people from engaging in such conduct.[81]

The adequacy of penalties for cyberbullying

3.56 The Attorney-General's Department explained a general approach to setting maximum penalties:

> The maximum penalty applied to an offence should aim to provide an effective deterrent to the commission of the offence and reflect the seriousness of the offence within the relevant legislative scheme. A higher maximum penalty will be justified where there are strong incentives to commit the offence or where the consequences of the commission of the offence are particularly dangerous and damaging.[82]

3.57 As discussed in Chapter 2, the committee heard evidence regarding the severe harms that cyberbullying can cause.

3.58 Victorian Women Lawyers submitted that '…social media platforms are now being used as a tool in cases of gender-based violence, and in particular, to perpetrate sexual violence, humiliation or harassment against women.' While acknowledging difficulties in setting penalties, it argued that'…it is imperative that the penalty acts as a deterrent.' Victorian Women Lawyers '…encourages consideration of whether the severity of the penalty is achieving appropriate outcomes, especially having a deterrent effect, to protect the vulnerabilities of women and young girls.'[83]

3.59 The Mental Health Commissions of Australia noted that many state and territory offences that could apply to cyberbullying carry maximum penalties greater than three years' imprisonment. It stated that '[i]n severe cases of cyberbullying, it is likely that a victim would take action under their state's relevant bullying laws…' rather than under section 474.17 of the Commonwealth Criminal Code. The Mental Health Commissions submitted that:

---

80 Maurice Blackburn Lawyers, *Submission 29*, p. 3.

81 AUARA, *Submission 1*, pp. 2–3.

82 Ms Harmer, Attorney-General's Department, *Committee Hansard*, 7 March 2018, p. 48; also see, for example, Tasmanian Government, *Submission 19*, p. 4.

83 Victorian Women Lawyers, *Submission 5*, pp. 4–5.

> [c]onsideration may be given regarding provisions that recognise the degree of harm that has resulted, including both physical and mental harm with, possible consideration to an escalating penalty.[84]

3.60 Both the Law Council and the Attorney-General's Department highlighted that harm caused to the victim can already considered during sentencing.[85]

3.61 The Law Council cautioned against introducing an aggravated offence related to harm caused to the victim. It argued that '…such an offence would be unduly difficult to prove and would likely result in greater trauma for the victim of the offence.'[86] However, the Law Council '…would not oppose…' increasing the maximum penalty, as long as the increased penalty did not exceed five years' imprisonment. It argued that:

> [m]ore serious offences such as using a carriage service to make a threat to kill (section 474.15) or using a carriage service to make a hoax threat (section 474.16) carry a maximum penalty of 10 years imprisonment. Using a carriage service to make a threat to cause serious harm (s474.17(2)) carries a maximum penalty of 7 years imprisonment. It would seem, then, that there is adequate scope to increase the maximum penalty for a section 474.17 offence to, say, five years imprisonment, whilst still maintaining adequate distinction from the more serious offences outlined.[87]

3.62 Noting the complexities of cyberbullying between children, Ms Podesta of the Alannah & Madeline Foundation argued that:

> …if there were any criminal definition in an attempt to look at legislation, overwhelmingly we would say that there needs to be a very low level of penalties attached it, apart from the most excessive of cases…some of the worst instances of cyberbullying take place with adults…Some of the instances with children are about things that would never get anywhere near the level of criminal behaviour and are more about behavioural and educational things.[88]

3.63 The NT Police submitted that the maximum penalty '…could be subject for review and increase, particularly when considering the actual and potential impacts.'[89] In addition, NT Police submitted that:

> …the penalty for section 474.17 fails to meet the serious offence test under the *Telecommunications (Interception and access) Act 1979* limiting the scope for using data interception techniques to progress these investigations.[90]

---

84 Mental Health Commissions of Australia, *Submission 9*, pp. 2–3.

85 Law Council, *Submission 15*, p. 13; Attorney-General's Department, *Submission 21*, p. 8.

86 Law Council, *Submission 15*, p. 13.

87 Law Council, *Submission 15*, p. 14.

88 Ms Podesta, Alannah & Madeline Foundation, *Committee Hansard*, 9 February 2018, p. 24.

89 Northern Territory Police Force, *Submission 22*, p. 2.

90 Northern Territory Police Force, *Submission 22*, p. 2.

3.64 However, the Attorney-General's Department said that '…telecommunications data, including an IP address…can be obtained for criminal matters, which would include an offence such as [section] 474.17.'[91]

91 Ms Harmer, Attorney-General's Department, *Committee Hansard,* 7 March 2018, p. 52.

Chapter 4

Social media platforms and other preventative measures

4.1 This chapter examines how cyberbullying could be addressed other than through criminal offences. It examines the evidence the committee received regarding:

- social media platforms, including their policies, procedures and practices; and
- education and prevention initiatives.

The policies, procedures and practices of social media platforms

4.2 As discussed in Chapter 2, the committee heard a great deal of evidence about the concerning prevalence of cyberbullying, and the significant harm it can cause to victims and those around them.

4.3 Several submitters posited that social media platforms have a role to play in addressing cyberbullying.[1] Some submitters also reported that social media platforms sometimes respond to complaints slowly or inadequately.[2] For instance, Ms Jenna Price, Committee Member, Women in Media, explained that:

> Sometimes you can complain about something that has happened to you on social media and it takes days. It depends. If your group has a strong connection with Facebook in Sydney, you can get help, but that's not available to everybody and sometimes it's not available even to the people who already have established that relationship…And then if they don't agree with you then you have to appeal, and that takes more time, and in the meantime your image, in whatever version it is, has been plastered all around the internet.[3]

4.4 The committee heard evidence from Facebook, Instagram, and the Digital Industry Group Incorporated (DIGI). Each of these organisations highlighted that

---

1 See, for example, Law Council of Australia (Law Council), *Submission 15*, pp. 16–18; Media, Entertainment & Arts Alliance (MEAA), *Submission 28*, pp. 5–6; Professor Marilyn Campbell, Founding Member, Australian Universities' Anti-bullying Research Alliance (AUARA), *Committee Hansard*, 9 February 2018, p. 1; Mrs Liza Davis, Director of Strategic Communications and Government Relations, ReachOut Australia, *Committee Hansard*, 7 March 2018, p. 29.

2 See, for example, Northern Territory Police Force, *Submission 22*, p. 2; Women in Media, *Submission 26*, p. 13; Miss Hayley Chester, Law Reform Committee Co-Chair, Victorian Women Lawyers, *Committee Hansard*, 9 February 2018, p. 18; Mr Josh Bornstein, Principal, Maurice Blackburn Lawyers, *Committee Hansard*, 7 March 2018, p. 2; Ms Terese Edwards, Chief Executive Officer, National Council of Single Mothers and their Children, *Committee Hansard*, 7 March 2018, p. 27.

3 Ms Jenna Price, Committee Member, Women in Media, *Proof Committee Hansard*, 9 February 2018, p. 35.

social media platforms operate under terms of service or 'Community Guidelines'.[4] DIGI further explained that:

> …across the industry, we have:
>
> - policies that prescribe how old you must be to use our services
> - policies that outline what can and cannot be shared via our services
> - tools that allow any of the millions of people who use our services to flag content to us that may violate our policies;
> - we invest in tools that can provide additional protections for minors, and
> - we invest in a reporting infrastructure that allows us to promptly review and remove any such content.[5]

4.5 The Law Council of Australia (Law Council) raised a number of issues with the operation of Facebook's 'Statement of Rights and Responsibilities' (Statement). These included whether an Australian minor is capable of agreeing to the Statement, and therefore whether the Statement is legally binding.[6]

4.6 Facebook submitted that '[o]ur content policies have been developed with the goal of allowing people to expressly themselves freely whilst also ensuring that people feel safe and respected.'[7] Ms Nicole Buskiewicz, Managing Director at DIGI, argued:

> We have an interest, as an industry, to ensure that the online space is a safe and respectful place. We want to ensure that people who are using our services are having a positive experience online.[8]

4.7 The committee also heard that social media platforms are implementing specific tools to improve safety for users. Ms Julie de Bailliencourt, Head of Global Safety Outreach at Facebook, stated that '…the way technology is evolving is exciting and offers a lot of possibilities that will help complement the notice-and-take-down system…'.[9] Ms de Bailliencourt provided some examples, including that Facebook checks 80 data points when a new account is created to identify whether or not it is a fake. She also stated that:

> …we have recently launched, in December, two anti-harassment tools, one in Messenger and one on Facebook, that will basically leverage the signal that we get from you. So, if you were blocking somebody on Facebook, and if we had any indication that this person had created, let's say, a new

---

4 Instagram, *Submission 3*, p. 2; Facebook, *Submission 4*, p. 2; Digital Industry Group Incorporated (DIGI), *Submission 17*, p. 2.

5 DIGI, *Submission 17*, p. 2.

6 Law Council, *Submission 15*, pp. 16–17.

7 Facebook, *Submission 4*, p. 2; also see Instagram, *Submission 2*, p. 1.

8 Ms Nicole Buskiewicz, Managing Director, DIGI, *Committee Hansard*, 9 February 2018, p. 46.

9 Ms Julie de Bailliencourt, Head of Global Safety Outreach, Facebook, *Committee Hansard*, 9 February 2018, p. 43.

> account or a similar, duplicate account, with the view to harass you, we have established with high certainty that we can block those other accounts without you having to do anything. We call this the super-block.[10]

The role of the eSafety Commissioner

4.8 As discussed in Chapter 1, the eSafety Commissioner has various powers to address cyberbullying material targeting an Australian child. The eSafety Commissioner explained that:

> [a]s an office, we also work closely with social media sites to get the cyberbullying material taken down. Thus far, we've had a 100 per cent compliance rate and so have not had to use our formal powers. And we are reaching out proactively to a broad range of online services and app providers to make sure that they're in compliance with the scheme.[11]

4.9 The Office of the eSafety Commissioner (eSafety Office) submitted that '[o]n balance, the Commissioner considers that the policies, procedures and practices of the large social media services to address cyberbullying are working.'[12] However, it also submitted that its role '…is to offer a safety net when a social media services does not consider a report made to them under their reporting tool to amount to a breach of their terms of use.'[13] As the eSafety Commissioner explained:

> …it's written into the provisions that the child, or the parent or guardian must report to the social media sites initially. As Nicole [Buskiewicz, Managing Director at the Digital Industry Group Incorporated] said, that's the most expeditious way of getting that down in the first instance. But if the content doesn't come down within 48 hours, they can come to us. The role we play as a safety net is that a lot of the moderators, depending on the platform, may have 30 seconds or a minute to look at the reports as they come in. They're dealing with huge volumes and they often miss context. What the young people that report to us can do is give us that context and we can make a case on their behalf and advocate on their behalf. That's why we have had success with the 700 cases we've brought down. There have been very few times when the social media sites say 'You determined that this was serious cyberbullying, we're going to contest you on this.'[14]

4.10 Ms Buskiewicz highlighted that '…no civil penalties have been levied under the scheme since it started'. She argued:

> This is because the robust and well-established report-and-take-down systems that members have had in place for over a decade leading up to the establishment of the eSafety office allow them to effectively and

---

10 Ms de Bailliencourt, Facebook, *Committee Hansard*, 9 February 2018, p. 43.

11 Ms Julie Inman Grant, eSafety Commissioner, Office of the eSafety Commissioner, *Committee Hansard*, 9 February 2018, p. 61.

12 Office of the eSafety Commissioner (eSafety Office), *Submission 13*, p. 8; also see Ms Inman Grant, eSafety Commissioner, *Committee Hansard*, 9 February 2018, p. 62.

13 eSafety Office, *Submission 13*, p. 7.

14 Ms Inman Grant, eSafety Commissioner, *Committee Hansard*, 9 February 2018, p. 62.

> expeditiously resolve complaints. With or without civil and criminal laws, we will continue to do this.[15]

4.11 However, the eSafety Office also noted that there is room for improvement:

> Social media services champion community standards, rules and basic norms of behavior on their platforms. However, sometimes the services fall short of evolving these policies in response to malfeasance they are witnessing on their platforms, and in ultimately enforcing these norms. The Commissioner would like to see better policing of conduct by providers, as a clear demonstration that they intend to be held to their published policies. The Office understands that safety is a journey – not a final destination – and we will continue to work with social media providers to share online abuse trends and to encourage them greater innovation and investment in safety protections.[16]

4.12 When asked whether legislative changes might make the eSafety Office more effective in addressing cyberbullying, the eSafety Commissioner stated that '[w]e found the act quite workable, and our discretionary powers are quite broad.'[17]

4.13 The eSafety Office cited some challenges in applying its end user notice scheme in cases where the perpetrator's identity cannot be established from public records. It stated that in order to access social media account data from a platform hosted in the USA, a formal court or treaty process is generally required. This process is most effective if a request to the service to preserve the relevant data has already been made. The eSafety Office stated that there may be merit in the office being able to reach a formal arrangement with the Australian Federal Police (AFP) in which the AFP makes preservation requests on behalf of the Office. The eSafety Office could then manage the court process.[18]

4.14 The Law Council expressed support for the eSafety Commissioner's two-tier scheme, but recommended some changes.[19] First, it recommended that the Tier 2 scheme be expanded to allow small service providers to be declared as Tier 2. Second, it highlighted that a social media platform's Tier 1 status can only be revoked (and replaced with Tier 2 status) if 12 months has passed since it became a Tier 1 service. The Law Council argued that '[t]his is a long period in which serious consequences could occur from cyberbullying.' It recommended that:

> …the eSafety Commissioner be given a discretion to remove a service's 'tier 1' status after a shorter period of time, if the provider has clearly failed to remove material that has potentially serious consequences.[20]

---

15 Ms Buskiewicz, Managing Director, DIGI, *Committee Hansard*, 9 February 2018, p. 41.

16 eSafety Office, *Submission 13*, p. 9.

17 Ms Inman Grant, eSafety Commissioner, *Committee Hansard*, 9 February 2018, p. 64.

18 eSafety Office, correspondence received 23 March 2018, p. 1.

19 Law Council, answers to questions on notice, 9 February 2018 (received 5 March 2018), p.4.

20 Law Council, *Submission 15*, pp. 20–21.

4.15 The eSafety Office raised the possibility of increasing the basic online safety requirements under the *Enhancing Online Safety Act 2015* (Online Safety Act) to require '…robust user settings and terms of use, clear and unequivocal community standards, and a proactive approach to dealing with cyberbullying on the platform.'[21]

4.16 The Australian Women Against Violence Alliance submitted that the work of the eSafety Commissioner should be extended to focus not only on cyberbullying directed at children but also on other groups at risk.[22] The eSafety Commissioner also stated that this idea may have merit, noting that the eSafety Office has received a growing number of complaints from adults since its remit was expanded to include all Australians.[23] The relevant groups of vulnerable adults could include people with disability, Aboriginal and Torres Strait Islander people, people who identify as LGBTIQ, women experiencing domestic violence, and people with a non-English speaking background.[24] The eSafety Commissioner noted that any extension of the scheme '…should come with additional resourcing.'[25]

4.17 Additionally, the eSafety Commissioner expressed concern that the definitions of 'social media service' and 'relevant electronic service' under the Online Safety Act are not sufficiently clear and do not adequately capture gaming platforms or anonymous social interaction apps such as Sarahah.[26] The eSafety Office stated that it would be useful to amend these definitions so that the eSafety Office could bring these kinds of platforms into the tier scheme.[27]

A duty of care for social media platforms

4.18 Mr Josh Bornstein, Principal at Maurice Blackburn Lawyers, supported a publicly funded regulator to monitor and investigate cyberspace issues and safety breaches. But he also stated that the regulator would be unable to manage all cyberbullying cases because '…cyberspace is enormous…'. He proposed:

> …empowering individuals, whether they are journalists who are targeted and trolled or whether they are the parents of children who are bullied online, to take legal action against Google, against Facebook and against Twitter for, in effect, breaching their duty of care.[28]

4.19 Mr Bornstein argued that this would:

---

21 eSafety Office, correspondence received 23 March 2018, p. 4.

22 Australian Women Against Violence Alliance, *Submission 14*, p. 2.

23 eSafety Office, correspondence received 23 March 2018, p. 4.

24 eSafety Office, correspondence received 23 March 2018, p. 4.

25 eSafety Office, correspondence received 23 March 2018, p. 4; Australian Women Against Violence Alliance, *Submission 14*, p. 2.

26 eSafety Office, correspondence received 23 March 2018, p. 4.

27 eSafety Office, correspondence received 23 March 2018, pp. 1–2.

28 Mr Bornstein, Maurice Blackburn Lawyers, *Committee Hansard*, 7 March 2018, p.1.

> …provide a very strong financial incentive to the big social media companies to clean up their act. In the same way that we provide strong financial incentives to employers and to occupiers of premises—to supermarkets—to make sure that their premises are safe when people use them, we should require Facebook, Google and others to take all practicable and reasonable steps to ensure that their sites are safe for users as well.[29]

4.20 Some other witnesses agreed that this kind of model is at least worthy of consideration.[30] Ms Van Badham of the Media, Entertainment & Arts Alliance stated:

> I agree with Josh Bornstein's position, that there has to be a duty of care. Coming from professional media anyway, if a publication, *The Guardian*, *The Australian*, Fairfax, if any of the major media organisations in this country were facilitating the harassment and abuse of individuals, they would be held accountable. Social media are media corporations. Facebook is effectively a modern newspaper. So is Twitter. It has a pretty loose content policy, but those platforms exist as publication vehicles, and they must take responsibility for the care of participants within that.[31]

4.21 However, the submission from DIGI supported a contrary position:

> Given the strong commitment of industry to promote the safety of people when they use our services, we believe that no change[s] to existing criminal law is required. If anything, we would encourage the Committee to consider carve outs from liability for responsible intermediaries.[32]

4.22 Additionally, Ms Mia Garlick, Director of Policy, Australia & New Zealand, Facebook and Instagram, was asked about legal liability for social media platforms. She stated that '…regulations are clearly a matter for the government. But from our perspective, regulation isn't what motivates us; it's the consumer experience.'[33] Facebook and Instagram also stated that:

> [o]n Facebook, people choose who to be friend with, and which Pages or Groups to follow. Consequently, people make a decision about the types of content that they can see in their News Feed. News Feed then ranks the stories based on how relevant a particular piece of content is that a person has chosen to see. We do not write the posts that people read on our services.

---

29 Mr Bornstein, Maurice Blackburn Lawyers, *Committee Hansard*, 7 March 2018, pp.1–2.

30 See, for example, Mr Adam Portelli, Director, Victorian Branch, MEAA, *Committee Hansard*, 7 March 2018, p. 10; Ms Sonya Ryan, Chief Executive Officer and Founder, Carly Ryan Foundation, *Committee Hansard*, 7 March 2018, pp. 20–21; Ms Edwards, National Council of Single Mothers and their Children, *Committee Hansard*, 7 March 2018, p. 27.

31 Ms Van (Vanessa) Badham, Media Section Vice President, Victorian Branch, MEAA, *Committee Hansard*, 7 March 2018, p. 13.

32 DIGI, *Submission 17.1*, p. 2.

33 Ms Mia Garlick, Director of Policy, Australia & New Zealand, Facebook and Instagram, *Committee Hansard*, 9 February 2018, p. 47.

> While we are not in the business of picking which issues the world should read about, we are in the business of connecting people and ideas — and matching people with the stories they find most meaningful.[34]

4.23 The Law Council clarified that existing positive obligations under the *Telecommunications Act 1997* '…will generally not be applicable to social networking sites, as they are not carriage service providers.' However, the obligations may apply to the direct messaging applications of social media platforms, because '…these messaging applications…may be regulated carriage service providers and hence caught by the Telecommunications Act obligations.'[35]

4.24 Additionally, the Law Council referred to the civil penalty regime that already exists under the Online Safety Act and is administered by the eSafety Commissioner. The Law Council noted that civil penalties have not yet been applied to social media platforms, and that the eSafety Commissioner reports largely positive experiences with social media platforms. It submitted that it:

> …does not consider that there has been a demonstrated need at this time to impose a positive obligation by way of a criminal penalty on social media services to remove cyberbullying content from their platform.[36]

Safety by design

4.25 Safety by design is '…the notion that safety ought to be built-in to social media services from the outset as a fundamental and core principle of design.'[37] The eSafety Commissioner strongly supports this approach, and her office submitted that:

> [t]he Commissioner considers it is reasonable to expect that large social media services should proactively adopt a 'safety first' approach to engineering their platforms and features, much as they have already done with 'security by design' and 'privacy by design'.[38]

4.26 The eSafety Office provided some positive examples of this, including:

- the Lego Life children's social networking app, which employed '…trained moderators to enforce an extensive code of conduct for users'; and
- Snap, Inc. requiring '…users to deliberately opt-in to the Snap Map feature, rather than opt-out.'[39]

4.27 The eSafety Commissioner also noted a negative example, Facebook Live:

---

34 Facebook and Instagram, answers to questions on notice, 9 February 2018 (received 7 March 2018), p. 4.

35 Law Council, answers to questions on notice, 9 February 2017 (received 5 March 2018), pp. 3–4.

36 Law Council, answers to questions on notice, 9 February 2017 (received 5 March 2018), pp. 4–5.

37 eSafety Office, *Submission 13*, p. 8.

38 eSafety Office, *Submission 13*, p. 8.

39 eSafety Office, *Submission 13*, p. 8.

> When Facebook Live went live, it took about a dozen murders, suicides and rapes on Facebook Live for them to say, 'We're going to hire 3,000 moderators,' yet Periscope and Meerkat had been out in the market for some time, so they could have reasonably anticipated that there would be some safety issues requiring moderation.[40]

4.28 The Alannah & Madeline Foundation submitted that '…the "start-up" (innovation) culture of the technology industry prioritises "testing in the marketplace" and responding to user feedback to improve their services – this takes precedence over "user safety by design".'[41] Further, new start-up platforms:

> …can often have significant cyberbullying and harassment issues, due to their lack of monitoring and reporting processes. Young people are often the "play-testers" in this environment, as their age group has a higher proportion of "early adopters".[42]

4.29 The eSafety Commissioner stated that one role her office would like to play is to '…encourage companies to put safety by design first' and to '…develop and implement stronger policies and enforcement procedures.'[43] She also noted the difficulties of legislating on safety by design:

> I think that would be very hard to implement. Technology is always going to outpace public policy. I imagine any legislator would have a hard time anticipating where the newest technology might be or where it might go, and I don't think we want to stifle innovation.[44]

4.30 However, as the eSafety Commissioner stated:

> …if [social media platforms are] not responsive or don't acquiesce and they're active in our market and young people are being abused on them, that's when we can go to the minister's office and declare them a tier-2 player.[45]

Social media platforms and data

4.31 Some submitters stated that it may be beneficial for social media platforms to publish relevant data, including data about complaints received and the platforms' responses to them.[46] The National Children's Commissioner at the Australian Human Rights Commission stated that reporting on data:

---

40 Ms Inman Grant, eSafety Commissioner, *Committee Hansard*, 9 February 2018, p. 70.

41 Alannah & Madeline Foundation, *Submission 10*, p. 6.

42 Alannah & Madeline Foundation, *Submission 10*, p. 6.

43 Ms Inman Grant, eSafety Commissioner, *Committee Hansard*, 9 February 2018, p. 70.

44 Ms Inman Grant, eSafety Commissioner, *Committee Hansard*, 9 February 2018, p. 70.

45 Ms Inman Grant, eSafety Commissioner, *Committee Hansard*, 9 February 2018, p. 70.

46 See, for example, UNSW Law Society Inc., *Submission 34*, p. 4; Ms Ginger Gorman, Committee Member, Women in Media, *Committee Hansard*, 9 February 2017, p. 35.

> …provides the social media providers an opportunity to enhance their education by demonstrating what they're doing in this space. If they've got a good story to tell, I think they should be telling it.[47]

4.32 Ms Buskiewicz of DIGI said that the data on complaints vary, and stated:

> The member company policies vary on whether they release those numbers. The example I can give is YouTube, which receives 275,000 flags a day for review across all types of content, and that is in the context of having 400 hours of video content uploaded to YouTube every day. So there is a real volume of content that goes up.[48]

4.33 Ms Buskiewicz stated that she did not have this data for Australia only.[49]

4.34 In answering questions on notice, Facebook and Instagram stated that '[w]e understand the rationale behind your requests for us to provide more detail around the data showing reporting trends, however, unfortunately at this stage, we are not able to do so.'[50] However, Facebook and Instagram also highlighted methods of removing content before users report it to them. For instance, they stated that:

> …we use automation, image matching and other tools to proactively identify and remove 99% of the terror-related content before anyone in our community has flagged it to us, and in some cases, before it goes live on the site.[51]

4.35 Ms de Bailliencourt of Facebook also said that complaint wait times vary, but '[t]he vast majority…' are reviewed within 24 hours, and '[s]ome may go to 48 hours.' She explained that '[w]e try to go even faster on very sensitive reports, such as bullying. Suicide prevention is the one we try to get to in minutes—when we're very good.'[52]

4.36 The eSafety Office told the committee that between 1 October 2017 and 31 January 2018, the '…average length of time between the Office requesting removal of content from a social media service, to the Office being informed that the material has been removed, was 39 hours.' It stated that '[i]n the majority of cases, material will have been removed well before notification.' In addition, '[t]he fastest time for

---

47 Ms Megan Mitchell, National Children's Commissioner, Australian Human Rights Commission, *Committee Hansard*, 9 February 2018, p. 58.

48 Ms Buskiewicz, Managing Director, DIGI, *Committee Hansard*, 9 February 2018, p. 47.

49 Ms Buskiewicz, Managing Director, DIGI, *Committee Hansard*, 9 February 2018, p. 47.

50 Facebook and Instagram, answers to questions on notice, 9 February 2018 (received 7 March 2018), p. 2 and p. 3.

51 Facebook and Instagram, answers to questions on notice, 9 February 2018 (received 7 March 2018), p. 2.

52 Ms de Bailliencourt, Head of Global Safety Outreach, Facebook, *Committee Hansard*, 9 February 2018, p. 50.

content removal by a social media service following a request by the Office was 26 minutes.'[53]

4.37 Facebook and Instagram informed the committee that:

> [w]e now have around 14,000 people working across community operations, online operations, and our security efforts. We are committed to increasing this number across all of these teams to a total of 20,000 by 2018.[54]

4.38 The eSafety Commissioner stated that, based on her industry experience, social media moderators have a very short time to consider complaints:

> It is 30 seconds to a minute. It may vary. You would have to verify that with Facebook…Most of the social media sites have triaging functions. So, depending on which boxes you tick, they'll be able to determine—if it's image based abuse it may go to one queue, versus child sexual exploitation versus bullying, or 'this comment was inappropriate'.[55]

4.39 The eSafety Office submitted that from 1 October 2018 to 31 January 2018 it responded to 97 percent of all complaints about cyberbullying within three hours and resolved complaints, on average, in 150 minutes.[56]

4.40 The social media representatives at the hearing on 9 February 2018 were asked whether they would object to a law requiring platforms to publish data about complaints, broken down by category. Ms Buskiewicz of DIGI said:

> We need to ask: what are we trying to get from the numbers? If we're talking about incentivisation, that's only one way. As Mia [Garlick of Facebook and Instagram] said before, we are very much reliant on feedback and we're continually striving to do better, and we will do that regardless of whether we have to publish numbers.[57]

4.41 Ms Garlick of Facebook and Instagram argued that published data '…might not be clear as to what it's showing', and added:

> It's up to you guys to make recommendations and decisions on the law. From our perspective, that's not going to be what motivates us to make sure we're doing the best we can to remove the content as fast as we can.[58]

4.42 The eSafety Office stated that the publication of this kind of data would be beneficial, but also acknowledged that the data's usefulness would be limited:

---

53 eSafety Office, answers to questions on notice, 9 February 2018 (received 7 March 2018), p. 2.

54 Facebook and Instagram, answers to questions on notice, 9 February 2018 (received 7 March 2018), p. 4.

55 Ms Inman Grant, eSafety Commissioner, *Committee Hansard*, 9 February 2018, p. 70.

56 eSafety Office, answers to questions on notice, 9 February 2018 (received 7 March 2018), p. 3.

57 Ms Buskiewicz, Managing Director, DIGI, *Committee Hansard*, 9 February 2018, p. 48.

58 Ms Garlick, Facebook and Instagram, *Committee Hansard*, 9 February 2018, p. 48.

> Data about cyberbullying and other abuses collected by the social media services would be useful to have. For example, the information might be used to target resources, raise awareness, and provide education on specific issues.
>
> However, it is unclear how much weight we could place on this type of information. There are two reasons for this. The first is that user-flagging of objectionable material on a service will always rely on the specific rules, guidelines or standards applicable to that service, rather than the statutory thresholds employed by the eSafety Commissioner. The second is that the data, being user-generated and unverified, may not reliably reflect the actual incidence of cyberbullying on a platform.[59]

Education and prevention

4.43 A large number of submitters and witnesses, including government agencies responsible for children and education, emphasised the importance of education in addressing cyberbullying.[60] As the Australian Government Department of Education and Training (Department of Education) submitted:

> In dealing with cyberbullying, the department supports a whole-school, systemic approach that emphasises early intervention and provides tiered levels of support for school children and young people affected by the negative behaviour. Measures should be age-appropriate and child focused, working with the person being targeted, their family and school, social media services, the perpetrator and when appropriate the police to address the issue.[61]

4.44 The Department of Education also provided details on how the Australian Curriculum addresses cyber safety and security both explicitly and implicitly from Foundation to Year 10.[62]

4.45 However, the eSafety Commissioner stated that '…there isn't consistent and comprehensive online safety education. Some schools do it really well; some schools totally miss the boat.' She explained that the eSafety Office has:

> …a certified online safety provider program, where I believe there are about 127 presenters from 27 different organisations—everyone from the

59 eSafety Office, answers to questions on notice, 9 February 2018 (received 7 March 2018), p. 1.

60 See, for example, Australian Government Department of Education and Training, *Submission 2*, p. 8; Queensland Family and Child Commission, *Submission 8*, p. 2; Mental Health Commissions of Australia, *Submission 9*, p. 2; Alannah & Madeline Foundation, *Submission 10*, p. 3; Western Australia Department of Education, *Submission 12*, p. 2; Australian Human Rights Commission, *Submission 16*, p. 3; DIGI, *Submission 17.1*, p. 1; Tasmanian Government, *Submission 19*, pp. 5–6; Women in Media, *Submission 26*, p. 12; ReachOut Australia, *Submission 31*, p. 2.

61 Australian Government Department of Education and Training, *Submission 2*, p. 4.

62 Australian Government Department of Education and Training, answers to questions on notice, 9 March 2017 (received 16 March 2016), p. 1.

> Carly Ryan Foundation and the Alannah & Madeline Foundation to PROJECT ROCKIT.[63]

4.46 Additionally, Ms Lesley Podesta, Chief Executive Officer at the Alannah & Madeline Foundation, posited that:

> [o]verwhelmingly—and this distresses me so much—it is a postcode lottery as to whether the teacher knows what to do. It's not because they don't care; it's because they have absolutely no resources or support about the most effective pathways to deal with it.[64]

4.47 The committee heard evidence regarding many existing initiatives and organisations offering education and support related to cyberbullying, including:

- Carly Ryan Foundation;[65]
- eSmart schools and eSmart libraries;[66]
- Kids Helpline;[67]
- Out of the Dark;[68]
- PROJECT ROCKIT;[69]
- ReachOut Australia;[70]
- Student Wellbeing Hub;[71]
- ThinkUKnow;[72]
- various initiatives cited by the Tasmanian Government,[73] and
- various initiatives cited by the Western Australia Department of Education.[74]

4.48 yourtown noted that children should not be the only focus of education initiatives:

---

63 Ms Inman Grant, eSafety Commissioner, *Committee Hansard*, 9 February 2018, p. 67.

64 Ms Lesley Podesta, Chief Executive Officer, Alannah & Madeline Foundation, *Committee Hansard*, 9 February 2018, p. 25.

65 Carly Ryan Foundation, *Submission 23*, p. 1.

66 Ms Podesta, Alannah & Madeline Foundation, *Committee Hansard*, 9 February 2018, p. 25.

67 yourtown, *Submission 6*, p. 3.

68 Queensland Family and Child Commission, *Submission 8*, p.2.

69 Instagram, *Submission 3*, p. 4; Facebook, *Submission 4*, p. 6.

70 ReachOut Australia, *Submission 31*, p. 2.

71 Australian Government Department of Education and Training, *Submission 2*, pp. 5–6.

72 Australian Federal Police, *Submission 18*, p. 1.

73 Tasmanian Government, *Submission 19*, p. 5–6.

74 Western Australia Department of Education, *Submission 12*, pp. 2–4.

> As with addressing other cyber safety concerns that confront our children and young people on a daily basis, such as sexting and pornography, government must recognise the importance, impact and potential value of the behaviour and responses of not just cyberbullying victims and perpetrators but also of bystanders, parents, teachers and wider support services.[75]

4.49 Indeed, the Queensland Family and Child Commission submitted, '[e]ducation initiatives must target adults as well as children and young people.'[76] The Australian Human Rights Commission also stated that '…parents are a critical target group for public awareness and support for children as they navigate online spaces…'.[77]

4.50 The committee heard that one important point for education and awareness initiatives is to encourage help-seeking behaviour. As Professor Barbara Spears of the Australian Universities' Anti-bullying Research Alliance stated:

> There's a stigma attached to seeking help. It means: 'I'm weak.' It means: 'I can't fix it myself.' We need to remember that young adolescents are of the age where they are trying to develop and identify as young, autonomous adults, and so they want to be seen to be solving problems themselves. So we have to give them the skills. We have to help them understand what help seeking means and how to go about looking for help and coping with bullying.[78]

4.51 The eSafety Commissioner cited her office's research, which '…tells us that young people are much less likely to use formal channels to seek support.' She stated that:

> [o]nly 50 per cent of young people turn to the family for assistance, around 13 per cent will involve their school and only 12 per cent report to a social media website. Fewer still, two per cent, report to the police.[79]

75 yourtown, *Submission 6*, p. 11.

76 Queensland Family and Child Commission, *Submission 8*, p. 4.

77 Australian Human Rights Commission, *Submission 16*, p. 3.

78 Professor Barbara Spears, Member, AUARA and Leading researcher, University of South Australia, *Committee Hansard*, 9 February 2018, p. 4.

79 Ms Inman Grant, eSafety Commissioner, *Committee Hansard*, 9 February 2018, p. 61.

Chapter 5

Committee view

5.1 Cyberbullying is a serious problem. It can cause severe harm to both victims and perpetrators, as well as their families, friends, and communities. It is critical that Australian governments, social media platforms, and broader society take action to reduce its incidence and the harm it causes.

5.2 The evidence gathered during this inquiry demonstrates that cyberbullying is extremely complex. There are myriad causes, and the consequences can vary greatly depending on context and the individuals concerned. Cyberbullying occurs in many guises, and there are major differences between cyberbullying by children and cyberbullying by adults.

5.3 A clear and agreed definition of cyberbullying, which acknowledges its complexity, would support effective policymaking. It would also make the issue clearer for the community, which is an important step in reducing the incidence of cyberbullying behaviours.

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.

5.5 The committee agrees with the weight of evidence that both bullying and cyberbullying are, at their roots, social and public health issues. Government measures to reduce cyberbullying should emphasise prevention and education. They should recognise that the causes of cyberbullying are linked to broader societal issues, including schoolyard bullying and sexism. They should also appreciate that some groups experience a disproportionate amount of cyberbullying.

5.6 The committee heard encouraging evidence about education initiatives, especially for young people, delivered both by government and non-government organisations. However, it appears that not all children, and perhaps many adults, are not properly exposed to these initiatives. The continued prevalence of cyberbullying indicates that further work is required.

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.

Criminal offences

5.8 The committee agrees that criminal offences should only be applied in the most serious cyberbullying cases. In general, other avenues to address the problem should be exhausted before criminal action is taken, particularly where the perpetrator is a child. The committee also acknowledges that criminal charges can only be applied after the damage has been done.

5.9 The committee accepts evidence that existing Commonwealth, state, and territory criminal offences adequately cover serious cyberbullying behaviours. In particular, section 474.17 of the *Criminal Code Act 1995* (Criminal Code) is a broadly framed, technologically-neutral offence.

5.10 Nonetheless, the committee is concerned by evidence implying that some cases of serious and possibly criminal cyberbullying have not been pursued in the courts. This may be due to a lack of awareness of the offences among the public. It may also be due to a lack of understanding of, or willingness to apply, these provisions by law enforcement authorities. It appears that there may be particular difficulties with how police currently investigate cyberbullying cases in which the perpetrator is anonymous, or in which multiple victims or perpetrators reside in different states or territories. The cases relayed by the National Council of Single Mothers and their Children (at paragraphs 3.43 to 3.44) were especially concerning.

5.11 The committee notes that law enforcement authorities currently do not employ adequate and consistent training across and within jurisdictions and that there is an urgent need to raise understanding and awareness of how existing criminal offences can be applied to cyberbullying behaviours. Further, it appears that the current problems may be compounded by differences between the relevant laws of states, territories, and the Commonwealth.

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.

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.**

5.14 The maximum penalties for cyberbullying should recognise the serious harm that cyberbullying can cause. This includes high levels of distress and mental health problems, and there may also be some degree of link between cyberbullying and suicide. The committee takes the view that the current maximum penalty under section 474.17 of the Criminal Code may not adequately recognise these harms, and is conscious that similar but more serious offences in the Criminal Code have maximum penalties of seven or ten years' imprisonment.

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 Office of the eSafety Commissioner

5.16 The committee strongly supports the role of the Office of the eSafety Commissioner, including the cyberbullying complaints scheme. The committee is conscious that the eSafety Office manages a very high number of cyberbullying complaints, and the total volume appears to be increasing. The team responsible for addressing these complaints comprises just four staff members. It is critical that the Australian Government provide adequate resources for the Office of the eSafety Commissioner to fulfil all its functions.

5.17 It is also important that the general public be aware of the eSafety Commissioner's work, and that victims of cyberbullying can make complaints to the Commissioner in certain circumstances. Cyberbullying remains common, and it is plausible that the large number of complaints received by the eSafety Commissioner each year does not include all meritorious cases.

5.18 Further, the committee considers it important that the Australian Government continually evaluate whether amendments to the eSafety Commissioner's functions and procedures, including the cyberbullying complaints scheme, would be beneficial.

5.19 The committee accepts evidence from the eSafety Office that the definitions of 'social media service' and 'relevant electronic service' under the *Enhancing Online Safety Act 2015* may not adequately capture all platforms on which cyberbullying occurs. Additionally, consideration should be given to increasing the basic online safety requirements for social media services under the Act. Consideration should also be given to improving the ability of the eSafety Office to work with the Australian Federal Police to access social media account data, and other relevant data, to improve its ability to apply the end user notice scheme.

5.20 The committee notes with interest the Law Council of Australia's recommendations (at paragraph 4.14) to amend technical elements of the cyberbullying complaints scheme. The committee also notes that the complaints scheme is currently limited to cyberbullying material targeting an Australian child, and agrees with evidence that it may be appropriate to expand the scope. This expansion could encompass vulnerable adults or all adults, but would require more resources to be allocated to the eSafety Office.

5.21 Additionally, the committee sees potential merit in requiring social media platforms to name and authorise a person to receive legal service in Australia, similar to the provisions of the Network Enforcement Act in Germany. The committee notes that the *Enhancing Online Safety Act 2015* currently requires Tier 1 services to name an employee as contact person for the purposes of that Act, which is a lesser requirement and does not apply to all social media platforms.

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, and**
- **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.**

Social media platforms

5.23 The committee acknowledges that the services provided by social media platforms are very often beneficial for individuals and society. However, these platforms are also a primary vehicle for serious cyberbullying.

5.24 The committee notes that civil penalties for social media platforms are already in place, but the eSafety Commissioner has not yet considered it necessary to apply them. This is partly due to cooperation from social media platforms. Given this, the committee does not think it is currently necessary to increase the maximum civil penalty that the eSafety Commissioner could apply.

5.25 However, the committee remains deeply concerned about the continued prevalence of cyberbullying on social media platforms. It is conscious that businesses are motivated by financial considerations, and sees merit in the proposal from Maurice Blackburn Lawyers (at paragraphs 4.18 to 4.19) to impose a statutory duty of care on social media platforms to ensure the safety of their users. It also encourages the

Australian Government to closely monitor the recently introduced Network Enforcement Law in Germany, and apply useful lessons from Germany in Australia.

5.26 Social media platforms should play a major role in reducing cyberbullying. The eSafety Commissioner's cyberbullying complaints scheme is a safety net and its existence does not reduce the responsibilities of Facebook, Google, Twitter and their ilk. The committee is deeply concerned about cases in which social media platforms appeared to respond inadequately to complaints, and wishes to make it clear that it is up to social media platforms to make their platforms safe environments, reduce the incidence of cyberbullying, and promptly take down or otherwise manage all offending material. The committee considers 'safety by design' a useful principle here.

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.

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.

5.29 The committee heard evidence regarding social media platforms' data, including data on user complaints, broken down by the type of complaint and the nature of the platform's response. The committee notes that the Network Enforcement Law in Germany contains certain reporting requirements. Notwithstanding the assurances of social media platforms, the committee considers that the mandatory publication of this data would provide considerable motivation for the platforms to address cyberbullying. This data would also aid society's understanding of the nature and scale of cyberbullying, although the committee acknowledges that user-generated data may have some limitations.

5.30 Given the Office of the eSafety Commissioner's role and expertise, it may be appropriate for the eSafety Commissioner to define what data must be published, and the format in which it must be presented.

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.

Senator Louise Pratt
Chair

ADDITIONAL REMARKS FROM GOVERNMENT MEMBERS

1.1 Government members of the committee are in agreement that there is no dispute about the harmful effects of cyberbullying on both children and adults. Similarly, Government members agree that bullying in any form represents a complex social phenomenon that cannot be reduced to a solely legal formulation.

1.2 Nonetheless, Government members are persuaded that the current legal mechanisms that capture cyberbullying behaviours did not contemplate such conduct at the time they were devised. Similar to the creation of legislative schemes to enhance and update relevant telecommunications law around the capture and storage of metadata as a result of the advent of widely available internet access, so too should some thought be given to the utility and cohesion of existing legal frameworks for cyberbullying. Government members would stress, however, that any legislative developments should be conducted in context of the social and cultural realities of these behaviours, particularly in the case of child perpetrators and victims.

1.3 Government members agree with recommendation 1 of the committee report – that state and territory governments and stakeholder bodies should work with the commonwealth to develop a clear definition of cyberbullying. Government members agree that the issue warrants a cross-jurisdictional approach that involves governments, stakeholders and communities in addressing the causes of, and potential remedies for, the problem of cyberbullying.

1.4 Government members agree in principle with Recommendation 2 of the committee report – that governments should acknowledge that cyberbullying is a social and public health issue and devise education initiatives accordingly.

1.5 Government members agree with Recommendation 3 – that the general public, and law enforcement agencies, be made fully aware of the scope of any applicable legislative schemes. Government members expect that such education would form part of the inevitable national conversation around the development of a revised legislative framework.

1.6 Government members do not agree with Recommendation 4 of the committee report – that the maximum penalty for 'using a carriage service to menace, harass or cause offence' under s474.17 of the Criminal Code Act 1995 should be increased from three years imprisonment to five years imprisonment. Government members are not currently persuaded that enhancing the punitive regime is the correct response to what is acknowledged widely to be a complex social issue. Government members suggest further consultation is required before committing to such action.

1.7 Government members of the committee agree with Recommendation 5 of the committee report – that the office, functions and procedures of the eSafety Commissioner should be enhanced.

1.8 Government members do not agree with Recommendation 6 of the committee report – that financial penalties, and other pressure, should be exerted by government

upon the operators of social media platforms regarding prevention of, and responsiveness to, cyberbullying. Government members expect that social media platform operators acknowledge the negative impacts of cyberbullying upon their business models and should be very willing to co-operate in such matters and should be consulted further.

1.9 Government members of the committee agree with Recommendation 7 of the committee report – that social media platforms should share information regarding cyberbullying with the eSafety Commissioner.

Senator the Hon. Ian Macdonald

Deputy Chair

Appendix 1

Public submissions

1 Australian Universities' Anti-bullying Research Alliance

2 Australian Government Department of Education and Training

3 Instagram

4 Facebook

5 Victorian Women Lawyers Association Inc

6 yourtown

7 National Council of Single Mothers & their Children

8 Queensland Family and Child Commission

9 Mental Health Commissions of Australia

10 Alannah & Madeline Foundation

11 Western Australia Police Force

12 Western Australia Department of Education

13 Office of the eSafety Commissioner

14 Australian Women Against Violence Alliance

15 Law Council of Australia

16 Australian Human Rights Commission

17 Digital Industry Group Incorporated

- 17.1 Supplementary to submission 17

18 Australian Federal Police

19 Tasmanian Government

20 Attorney-General’s Department

21 South Australian Government

22 Northern Territory Police Force

23 Carly Ryan Foundation

24 Confidential

25 Confidential

26 Women in Media

27 Confidential

28 Media, Entertainment & Arts Alliance

29 Maurice Blackburn Lawyers

30 Mr Andrew Jakubowicz

31 ReachOut

32 UNSW Law Society Inc.

33 The Hon. Shelley Hancock MP, Speaker of the NSW Legislative Assembly

34 Victims Of Abuse In The Australian Defence Force Association Inc

Additional information, answers to questions on notice and tabled documents

Additional information

1 Additional information provided by the Alannah & Madeline Foundation (received 9 February 2018).

2 Additional information provided by ReachOut Australia (received 7 March 2018).

3 Additional information provided by the Office of the eSafety Commissioner (correspondence, received 23 March 2018).

Answers to questions on notice

1 yourtown - answers to questions on notice taken at the public hearing on 9 February 2018 (received 16 February 2018).

2 Victorian Women Lawyers Association Inc - answers to questions on notice taken at the public hearing on 9 February 2018 (received 23 February 2018).

3 Law Council of Australia - answers to questions on notice taken at the public hearing on 9 February 2018 (received 5 March 2018).

4 Australian Universities' Anti-bullying Research Alliance - answers to questions on notice taken at the public hearing on 9 February 2018 (received 23 February 2018).

5 Facebook & Instagram - answers to questions on notice taken at the public hearing on 9 February 2018 (received 7 March 2018).

6 Office of the eSafety Commissioner - answers to questions on notice taken at the public hearing on 9 February 2018 (received 7 March 2018).

7 Queensland Mental Health Commission - answers to questions taken on notice by the National Mental Health Commission at the public hearing on 9 February 2018 (received 6 March 2018).

8 National Children's Commissioner, Australian Human Rights Commission - answers to questions on notice taken at the public hearing on 9 February 2018 (received 9 March 2018).

9 Carly Ryan Foundation - answer to question on notice taken at the public hearing on 7 March 2018 (received 14 March 2018).

10 Australian Government Department of Education and Training - answers to questions on notice taken at the public hearing on 7 March 2018 (received 16 March 2018).

11 National Council of Single Mothers & their Children - answer to question on notice taken at the public hearing on 7 March 2018 (received 15 March 2018).

Tabled documents

1 Document tabled by Instagram and Facebook at the public hearing on 9 February 2018 - opening statement (received 9 February 2018).

Appendix 2

Public hearings and witnesses

Friday, 9 February 2018 – Canberra

ANDREW, Dr Merrindahl, Program Manager, Australian Women Against Violence Alliance

BLACKMAN, Mr Jeremy, Senior Advisor, Cybersafety, Alannah & Madeline Foundation

BUSKIEWICZ, Ms Nicole, Managing Director, Digital Industry Group Inc.

CAMPBELL, Professor Marilyn, Founding Member, Australian Universities' Anti-bullying Research Alliance

CHESTER, Miss Hayley, Law Reform Committee Co-Chair, Victorian Women Lawyers

CLARKE, Ms Laura, Advocacy and Policy Lead, yourtown

DAGG, Mr Toby, Acting Manager, Compliance Tools and Citizen Services, Office of the eSafety Commissioner

DALGLEISH, Mr John, Head of Strategy and Research, yourtown

de BAILLIENCOURT, Ms Julie, Head of Global Safety Outreach, Facebook

D'SOUZA, Ms Vanessa, Acting Director, Policy, Analysis and Reporting, National Mental Health Commission

DWORJANYN, Miss Alex, Law Reform Committee Co-Chair, Victorian Women Lawyers

GARLICK, Ms Mia, Director of Policy, Australia & New Zealand, Facebook and Instagram

GORMAN, Ms Ginger, Committee Member, Women in Media

INMAN GRANT, Ms Julie, eSafety Commissioner, Office of the eSafety Commissioner

LOCH, Ms Liza-Jayne, National Committee Member, Women in Media

MITCHELL, Ms Megan, National Children's Commissioner, Australian Human Rights Commission

MOLT, Dr Natasha, Deputy-Director of Policy, Law Council of Australia

MOSES, Mr Arthur, SC, President-elect, Law Council of Australia

PODESTA, Ms Lesley, Chief Executive Officer, Alannah & Madeline Foundation

PRICE, Ms Jenna, Committee Member, Women in Media

SLEE, Professor Phillip Thomas, Member, Australian Universities' Anti-bullying Research Alliance

SPEARS, Professor Barbara, Member, Australian Universities' Anti-bullying Research Alliance; Leading researcher, University of South Australia

VASSILIADIS, Ms Maria, Executive Manager, Office of the eSafety Commissioner

Wednesday, 7 March 2018 – Melbourne

BADHAM, Ms Van (Vanessa), Media Section Vice President, Victorian Branch, Media, Entertainment and Arts Alliance

BORNSTEIN, Mr Joshua, Principal, Maurice Blackburn Lawyers

BUHAGIAR, Dr Kerrie, Director of Service Delivery, ReachOut Australia

CAMERON, Acting Commander Joanne Lee, Acting Manager Victim Based Crime, Australian Federal Police

CROSSLING, Detective Acting Superintendent Jayne, Acting National Coordinator, Missing Persons and Exploited Children, Australian Federal Police

DAVIS, Mrs Liza, Director of Strategic Communications and Government Relations, ReachOut Australia

EDWARDS, Ms Terese, Chief Executive Officer, National Council of Single Mothers and their Children

HARMER, Ms Anna, First Assistant Secretary, Security and Criminal Law Division, Attorney-General’s Department

MAHONEY, Detective Chief Inspector Dr Carlene, Strategic Coordinator, Youth and Crime Prevention Command, New South Wales Police Force

NATT, Ms Karina, Director, Corporate and Government Affairs, Carly Ryan Foundation

OAKLEY, Ms Jenna, Member, National Council of Single Mothers and their Children

PATTIE, Mr David, Group Manager, Improving Student Outcomes, Schools and Youth, Department of Education and Training

PORTELLI, Mr Adam, Director, Victorian Branch, Media, Entertainment and Arts Alliance

RYAN, Ms Sonya, Chief Executive Officer and Founder, Carly Ryan Foundation

SERRY, Ms Ella, Policy Officer, Student Inclusion Team, Improving Student Outcomes Group, Department of Education and Training

WARNES, Mr Andrew, Assistant Secretary, Communications Security and Intelligence Branch, Attorney-General’s Department