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.