Law Council
OF AUSTRALIA

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

Senate Legal and Constitutional Affairs Committee

20 October 2017

Telephone +61 2 6246 3788 • *Fax* +61 2 6248 0639
Email mail@lawcouncil.asn.au
GPO Box 1989, Canberra ACT 2601, DX 5719 Canberra
19 Torrens St Braddon ACT 2612
Law Council of Australia Limited ABN 85 005 260 622
www.lawcouncil.asn.au

Table of Contents

About the Law Council of Australia

The Law Council of Australia exists to represent the legal profession at the national level, to speak on behalf of its Constituent Bodies on national issues, and to promote the administration of justice, access to justice and general improvement of the law.

The Law Council advises governments, courts and federal agencies on ways in which the law and the justice system can be improved for the benefit of the community. The Law Council also represents the Australian legal profession overseas, and maintains close relationships with legal professional bodies throughout the world.

The Law Council was established in 1933, and represents 16 Australian State and Territory law societies and bar associations and the Law Firms Australia, which are known collectively as the Council's Constituent Bodies. The Law Council's Constituent Bodies are:

- Australian Capital Territory Bar Association
- Australian Capital Territory Law Society
- Bar Association of Queensland Inc
- Law Institute of Victoria
- Law Society of New South Wales
- Law Society of South Australia
- Law Society of Tasmania
- Law Society Northern Territory
- Law Society of Western Australia
- New South Wales Bar Association
- Northern Territory Bar Association
- Queensland Law Society
- South Australian Bar Association
- Tasmanian Bar
- Law Firms Australia
- The Victorian Bar Inc
- Western Australian Bar Association

Through this representation, the Law Council effectively acts on behalf of more than 60,000 lawyers across Australia.

The Law Council is governed by a board of 23 Directors – one from each of the constituent bodies and six elected Executive members. The Directors meet quarterly to set objectives, policy and priorities for the Law Council. Between the meetings of Directors, policies and governance responsibility for the Law Council is exercised by the elected Executive members, led by the President who normally serves a 12 month term. The Council's six Executive members are nominated and elected by the board of Directors.

Members of the 2017 Executive as at 1 January 2017 are:

- Ms Fiona McLeod SC, President
- Mr Morry Bailes, President-Elect
- Mr Arthur Moses SC, Treasurer
- Ms Pauline Wright, Executive Member
- Mr Konrad de Kerloy, Executive Member
- Mr Geoff Bowyer, Executive Member

The Secretariat serves the Law Council nationally and is based in Canberra.

Acknowledgement

The Law Council acknowledges the assistance of its National Criminal Law Committee, National Human Rights Committee, the Bar Association of Queensland and the Law Society of New South Wales in the preparation of this submission.

Executive Summary

1. The Law Council is pleased to provide this submission to the Senate Legal and Constitutional Affairs References Committee (**the Committee**) regarding its inquiry into 'The adequacy of existing offences in the Commonwealth Criminal Code and of state and territory criminal laws to capture cyberbullying' (**Inquiry**).

2. The Law Council strongly supports efforts to better ensure the online safety of children and adults. There are strong levels of community concern about the widespread nature of cyberbullying particularly given that it can cause significant psychological harm to victims. The Law Council emphasises however, 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.

3. In considering the adequacy of existing offences in the *Criminal Code Act 1995* (Cth) (**Criminal Code**) and of state and territory criminal laws to capture cyberbullying, the Law Council considers that the Australian Government needs have careful regard to certain guiding principles. These include a number of important human rights obligations as well as rule of law principles. Noting the tensions which may exist between the competing interests involved, the Australian response should seek to balance these interests in a manner which ensures that any limitations on individuals' rights are necessary, reasonable and proportionate.

4. The Law Council does not support the introduction of a new federal offence for broadcasting assaults and other crimes via social media platforms. It considers that existing offences in the Criminal Code and state and territory are adequate to capture a range of serious conduct which could constitute cyberbullying. The utilisation of a civil penalty regime, the eSafety Commissioner's powers and other less formal methods (be it school or mediation based) should be considered in less serious cases. Should this not be accepted and a new offence of broadcasting assaults and other crimes via social media platforms be introduced, the consent of the Attorney-General should be required before a person under the age of 18 could be charged with an offence. A penalty of 12 months imprisonment may be an appropriate penalty when compared with other telecommunications offences in the Criminal Code.

5. Further, the Law Council opposes any move to introduce an aggravated offence which is contingent upon harm to the victim. The *Crimes Act 1914* (Cth) (**Crimes Act**) already provides adequate scope for the harm to a victim to be considered in the sentence imposed. However, the Law Council would not oppose a general increase to the maximum penalty for a section 474.17 Criminal Code offence, provided it did not go beyond a maximum of 5 years imprisonment.

6. Additionally, the Law Council recommends that:

   (a) the recommendations of the Australian Law Reform Commission (**ALRC**) which emphasise the need for federal sentencing legislation to establish minimum standards for the sentencing of young offenders should be adopted to enhance sentencing practices for young cyberbullying offenders;

   (b) the Australian Government consider increased education and awareness of the possible consequences of cyberbullying, including criminal prosecution under the existing offences, for the community, law enforcement, prosecutors and the judiciary. Such messages should explain the application of these offences, and the relevant terminology, in a clear, accessible manner;

(c) the Australian Government should continue to work with social media sites to develop a best practice response to cyberbullying. This may include prioritisation of a parent's/guardian's complaint in relation to cyberbullying content;

(d) the eSafety Commissioner should be adequately resourced to effectively implement the existing civil penalty regime to target cyberbullying and other considerations such as the provision of counselling and other support for affected individuals;

(e) the eSafety Commissioner should be provided with greater flexibility regarding the range of appropriate penalties, enforcement mechanisms and other responses to deal with cyberbullying in the most appropriate manner;

(f) the distinction between tier 1 and tier 2 social media services in the *Enhancing Online Safety Act 2005* (Cth) (**Enhancing Online Safety Act**) should be maintained. However, the 12 month period in which a non-compliant tier 1 service is downgraded to a tier 2 service may be too long and may lead to serious consequences occurring from cyberbullying. The Law Council recommends 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; and

(g) the tier 2 enforcement scheme should be expanded to permit the Commissioner to enforce requests for removal of content from small service providers.

Cyberbullying

7. The definition of 'cyberbullying' is not universal and is open to debate.[1] The Office of the eSafety Commissioner defines cyberbullying as:

> *… the use of technology to bully a person or group with the intent to hurt them socially, psychologically or even physically.*[2]

8. The media for delivering cyberbullying can take a variety of forms and include 'the internet (personal websites, blogs, email), message boards or social networking sites, mobile phones using SMS or MMS, and online games'.[3]

9. There is a range of possible conduct which may constitute cyberbullying from harassment to cyberstalking. Other common types of behaviour include text-based name calling, use of coarse language, profanity and personal attacks (which may include racist or sexist attacks), 'flaming' (overt attacks), harassment or denigration, 'outing' of an individual's sexual preference or sending humiliating photos or video messages.[4]

10. Depending upon the severity of the conduct, a different kind of response – legislative or otherwise – may be required. Any analysis of proposals of the most appropriate responses to this issue also depends on whether the perpetrators of cyberbullying are children or adults. In the vast majority of cases, it may be that the perpetrators are children: in 2013 on average every two weeks an Australian parent reports an incident of cyberbullying to the police and Australian police had acknowledged a sharp rise in the number of such complaints.[5]

11. The Law Council considers that the development of an Australian Government response to cyberbullying issues needs to identify, and have careful regard to, certain key principles which are clearly relevant to discussions of how best to combat cyberbullying in Australia. This includes a number of human rights obligations, which have been voluntarily assumed by Australia under key international instruments, as well as particular rule of law principles.

Guiding human rights and rule of law principles

12. Identifying human rights obligations and rule of law principles at the outset may assist to identify the different interests involved in relation to cyberbullying, and to resolve in a principled manner the tensions which may arise when seeking to determine the most appropriate legislative responses.

13. While the list below is non-exhaustive, the Law Council considers that, in particular, the Australian Government's response should be framed in light of the human rights obligations set out below. These include, in particular, the rights of the child:

---

[1] Aashish Srivastava, Roger Gamble and Janice Boey, 'Cyberbullying in Australia: Clarifying the Problem, Considering the Solutions' (2013) 21 *International Journal of Children's Rights* 25, p. 27.
[2] E-Safety Commissioner, 'Cyberbullying', <https://esafety.gov.au/esafety-information/esafety-issues/cyberbullying>.
[3] Aashish Srivastava, Roger Gamble and Janice Boey, 'Cyberbullying in Australia: Clarifying the Problem, Considering the Solutions' (2013) 21 *International Journal of Children's Rights* 25, p. 27.
[4] Ibid, p. 28.
[5] Ibid, p. 37.

(a) to be ensured by the State such protection and care as is necessary for his or her wellbeing;[6]

(b) in all actions concerning the child, for his or her best interests to be a primary consideration;[7]

(c) to life, and to survival and development to the maximum extent possible;[8]

(d) where a child is capable of forming his or her own views, the right to express those views freely in all matters affecting him or her;[9]

(e) to freedom of expression. This right may be subject to certain restrictions, but only as provided by law and where necessary either for the respect of the rights or reputations of others; or the protection of national security, public order, public health or morals;[10]

(f) to freedom of association;[11]

(g) to privacy;[12] and

(h) to the highest possible standard of health.[13]

14. In discussions of cyberbullying, the above rights will carry a different resonance depending on whether the child involved is:

(a) a victim, or possible victim, of cyberbullying;

(b) a perpetrator, or possible perpetrator, of cyberbullying; or

(c) a bystander whose rights are nevertheless engaged in a possible cyberbullying incident (for instance, whose rights to privacy are engaged because of an investigation into online group communications).

15. In relation to a perpetrator who has been accused or charged with a criminal offence, the Law Council emphasises in particular the following principles, as set out in its *Detention Principles in the Criminal Law Context*:[14]

(a) in all actions concerning children, the best interests of the child shall be a primary consideration.[15]

---

[6] *Convention on the Rights of the Child* (**CROC**), adopted and opened for signature, ratification and accession by General Assembly Resolution 44/25, 20 November 1989 (entered into force 2 September 1990), Art 3.2.
[7] Ibid, Art 3.1.
[8] Ibid, Art 6.
[9] Ibid, Art 12.
[10] Ibid, Art 13.
[11] Ibid, Art 15.
[12] Ibid, Art 16.
[13] Ibid, Art 24.
[14] Law Council of Australia, *Detention Principles in the Criminal Law Context* (2013) <https://www.google.com.au/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwjQyeak0enWAhWHTrwKHcF1BYkQFggoMAA&url=https%3A%2F%2Fwww.lawcouncil.asn.au%2Fdocs%2Ffedf4ba5-af36-e711-93fb-005056be13b5%2F130622-Policy-Statement-Principles-Applying-to-Detention-in-a-Criminal-Law-Context.pdf&usg=AOvVaw0kA0mXgr05_mUybv1y4CpD> p. 5.
[15] CROC, Art 3.

(b) the arrest, detention or imprisonment of a child should be used only as a measure of last resort and for the shortest appropriate period of time.[16] Pre-trial detention of children should be avoided to the greatest extent possible.[17]

(c) every child accused of, or convicted of, a criminal offence should be treated in a manner which:

(i) is consistent with the promotion of the child's sense of dignity and worth;

(ii) reinforces the child's respect for the human rights and freedoms of others; and

(iii) takes into account the child's age, sex or gender and needs and the desirability of promoting the child reintegrating and assuming a constructive role in society.[18]

16. While the Inquiry appears to be mostly focused on cyberbullying by children or minors, the Law Council further notes the need to consider the rights of adults, such as those that appear in in the *International Covenant on Civil and Political Rights* (**ICCPR**), including:

(a) the right to be free from arbitrary or unlawful interference with a person's privacy, family, home or correspondence;[19]

(b) the right to freedom of expression;[20] and

(c) the right to freedom of association.[21]

17. The Law Council considers 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.

18. Further relevant principles which should be highlighted, and are relevant to the Law Council's consideration of these issues, include key rule of law principles such as:

(a) the law must be both readily known and available, and certain and clear. This means that the intended scope and operation of offence provisions should be unambiguous and key terms should be defined, so as to avoid dependence on police and prosecutorial discretion. In addition, the fault element for each element of an offence should be clear;[22] and

(b) executive decision making should comply with the principles of natural justice and be subject to meaningful judicial review.[23]

---

[16] CROC, Art 37(b); United Nations Standard Minimum Rules for the Administration of Juvenile Justice **(Beijing Rules)**, Rule 17 (see also Rule 11).
[17] Beijing Rules, Rule 13.
[18] CROC, Articles 37(c) and 40.1, see also Beijing Rules Rule 26.
[19] International Covenant on Civil and Political Rights opened for signature 16 December 1966, 993 UNTS (entered into force 3 January 1976) **(ICCPR),** Art 17.
[20] ICCPR, Art 19(2).
[21] ICCPR, Art 22.
[22] Law Council of Australia, *Policy Statement on Rule of Law Principles* (2011), Principle 1.
[23] Ibid, Principle 6.

The broadcasting of assaults and other crimes using social media platforms

19. The use of social media sites like Facebook and Instagram has become widespread with the rapid rise in the availability of mobile phones and internet access amongst the young. The incidence of the broadcasting of assaults and other crimes has also arisen, with the audience of such videos growing exponentially and with the broadcasting going 'viral'.[24]

20. As per the terms of reference for the Inquiry, a question arises as to whether the broadcasting of assaults and other crimes using social media platforms should be criminalised and whether such conduct is already captured under existing offences.

21. Section 474.17 of the Criminal Code (using a carriage service to menace, harass or cause offence) is one of the most relevant federal offences in the cyberbullying context.

22. Under subsection 474.17(1), a person is guilty of an offence if the person uses a carriage service[25] in a way that reasonable persons would regard as being, in all the circumstances, menacing, harassing or offensive. The maximum penalty for this offence is imprisonment for three years.

23. It is also an offence to attempt to use a carriage service in a way that reasonable persons would regard as being, in all the circumstances, menacing, harassing or offensive.[26]

24. Paragraph 474.17(1)(a) contains a physical element of conduct. By application of the default fault elements of section 5.6 of the Criminal Code, the fault element of intention will automatically apply. This means that a person must intentionally use the carriage service to be found guilty of the offence.

25. Paragraph 474.17(1)(b) contains a physical element of circumstance. The fact that the use of the carriage service occurs in a way that reasonable persons would regard as being, in all the circumstances, menacing, harassing or offensive constitutes a circumstance in which the offending conduct must occur. By application of the default fault elements in section 5.6, the fault element of recklessness will apply to a physical element of an offence that is a circumstance. 'Recklessness' as it applies to a circumstance is defined in section 5.4 of the Criminal Code; a person is reckless with respect to a circumstance if (a) he or she is aware of a substantial risk that the circumstance exists or will exist and (b) having regard to the circumstances known to him or her, it is unjustifiable to take the risk. Here, this means that an offender needs to be aware of a substantial risk that the use of the carriage service would be menacing, harassing or offensive to reasonable persons and having regard to the circumstances known to the offender it is unjustifiable to take the risk.

26. The authorities make it clear that, for the use of the carriage service to be criminally offensive, the degree of offensiveness must be serious.[27] It must involve more than mere hurt feelings on the part of a reasonable person.

---

[24] See for example, 'I'm a victim too: video bully,' *Sydney Morning Herald* (online), 22 March 2011, <http://www.smh.com.au/nsw/im-a-victim-too-video-bully-20110321-1c3u9.html>.
[25] 'Carriage service' is defined in section 7 of the *Telecommunications Act 2007* (Cth) as 'a service for carrying communications by means of guided and/or unguided electromagnetic energy'.
[26] *Criminal Code 1995* (Cth) s 11.1.
[27] *R v Monis* [2013] HCA 4 at [336].

27. Notwithstanding this limitation, many cases where crimes or assaults are broadcast would easily fall within the definition of section 474.17. In serious cases where a defendant broadcasts an abhorrent attack or a sexual assault on another person, a reasonable person would clearly be offended by that broadcast to the requisite standard. However, the provision may not so easily apply in other circumstances, which might be described as cyberbullying. For example, the broadcast of a schoolyard fight may not rise to the level of offense to a reasonable person or be regarded as harassing (in circumstances where it is simply posted on one occasion). Nevertheless, such use of a carriage service may be distressing to a person targeted by, or featuring in, the broadcast.

28. In those circumstances the Law Council appreciates the interest in enacting provisions to target the use of a carriage service to broadcast assaults or other criminal acts. However, the Law Council have concerns about how such a provision would be implemented and the consequences which may flow.[28]

29. The nature of cyberbullying, and social media generally, means that there is a high risk that a number of school-aged children would be caught by any proposed provision. Under the Crimes Act, a child under 10 years old cannot be liable for an offence against a law of the Commonwealth.[29] A child aged 10 years or more, but under 14 years old, can only be liable for an offence against a law of the Commonwealth if the child knows that his or her conduct is wrong.[30] The question whether a child knows that his or her conduct is wrong is one of fact. The burden of proving this is on the prosecution.[31]

30. The Law Council does not support the introduction of a new federal cyberbullying offence and considers that existing offences in the Criminal Code and state and territory are adequate to capture a range of serious conduct which could constitute cyberbullying.[32]

31. The Law Council considers that a key principle of the rule of law is that the law must be both readily known and available, and certain and clear.[33] This means that the intended scope and operation of offence provisions should be unambiguous and key terms should be defined, so as to avoid dependence on police and prosecutorial discretion.[34] In this respect, the Law Council is concerned that, if a new federal offence is introduced, depending upon the terminology used, there may be overlap of its

---

[28] The Law Council acknowledges the input from the Bar Association of Queensland for drawing many of the issues in this section to the Law Council's attention.
[29] *Crimes Act 1914* (Cth) s 4M.
[30] Ibid s 4N(1).
[31] Ibid s 4N(2).
[32] Existing Commonwealth offences include: *Criminal Code 1995* (Cth) ss 474.14 (using a telecommunications network with an intention to commit a serious offence), 474.15 (using a carriage service to make a threat to kill or cause harm to another person), 474.16 (using a carriage service for a hoax threat), 474.17 (using a carriage service to menace, harass or cause offence), and 474.29A (using a carriage service to transmit, make available, publish or otherwise distribute material that directly or indirectly counsels or incites suicide). Existing state and territory offences include *Crimes (Domestic and Personal Violence Act 2007* (NSW) s 13 (stalking or intimidation with intent to cause fear of physical or mental harm), *Crimes Act 1900* (NSW) ss 91P-91R (recording and distributing intimate images), *Crimes Act 199* (NSW) s 31 (documents containing threats), *Crimes Act 199* (NSW) s 199 (threatening to destroy or damage property), *Crimes Act 199* (NSW) s 60E (assaults etc at school), *Crimes Act 1958* (Vic) s 21A (stalking), *Crimes Act 1958* (Vic) s 20 (threat to kill), *Crimes Act 1958* (Vic) s 21 (threats to inflict serious injury), *Crimes Act 1900* (ACT) s 30 (threat to kill), *Crimes Act 1900* (ACT) s 31 (threat to inflict grievous bodily harm), *Crimes Act 1900* (Qld) s 308 (threats to murder in document), *Crimes Act 1900* (Qld) s 359 (threats), *Crimes Code 1913* (WA) ss 338A-338C (threats), *Crimes Act 1935* (SA) s 19 (unlawful threats), *Crimes Act 1924* (Tas) s 163 (threats to kill in writing) and *Crimes Code 1983* (NT) s 166 (threats constituted by words or conduct).
[33] Law Council of Australia, *Policy Statement on Rule of Law Principles* (2011), Principle 1.
[34] Ibid.

potential coverage with that under the existing offence under section 474.17. This is likely to lead to confusion about the likely scope and operation of the new offence versus the existing offence.

32. The utilisation of a civil penalty regime, the eSafety Commissioner's powers and other less formal methods (be it school or mediation based) should be considered in less serious cases.

33. Should this not be accepted and a new offence of broadcasting assaults and other crimes via social media platforms be introduced, the consent of the Attorney-General should be required before a person under the age of 18 could be charged with an offence. A provision such as this would ensure that only the most serious examples of alleged offending by children will be prosecuted and other less formal methods (be it school or mediation based) will be utilised in less serious cases.

34. Great care would also need to be taken in setting an appropriate maximum penalty for any proposed be offence. As discussed above, section 474.17 would apply to many more serious cases where a defendant broadcasts assaults or crimes. Accordingly, the maximum penalty for any new offence should necessarily be less than that which applies for section 474.17.

35. A 12 months imprisonment penalty may be an appropriate penalty when regard is had to other penalties for telecommunications offences in Division 474 of the Criminal Code.

Recommendations:

- **A new federal cyberbullying offence for broadcasting assaults and other crimes via social media platforms should not be introduced. The utilisation of a civil penalty regime, the eSafety Commissioner's powers and other less formal methods (be it school or mediation based) should be considered in less serious cases.**

- **Should this not be accepted and a new offence of broadcasting assaults and other crimes via social media platforms be introduced, the consent of the Attorney-General should be required before a person under the age of 18 could be charged with an offence. A penalty of 12 months imprisonment may be an appropriate penalty when compared with other telecommunications offences in the Criminal Code**

The application of section 474.17 and the adequacy of the penalties

36. The maximum penalty for an offence against section 474.17 is three years imprisonment.[35] This penalty was increased from the twelve-month maximum which applied to the predecessor provision (section 85ZE of the Crimes Act) when the provision was introduced in 2005.

37. As outlined above, there is a range of cyberbullying type of offences which would be covered by section 747.17. The Law Council appreciates that there will be occasions where offending against section 474.17 may cause a victim to self-harm or occasion other harm to a victim (aside from the obvious psychological harm). Further, it is appreciated that, as the use of technology and social media increases, the offending covered by section 474.17 may become more prevalent and, accordingly, a higher maximum penalty may be considered desirable in order to send the appropriate deterrent signal.

38. However, the Law Council would caution against any step which would see an 'aggravated' section 474.17 created based on harm to a victim. Subsection 16A(2) of the Crimes Act provides a non-exhaustive list of factors which a Court must take into account, generally, in sentencing an offender for a Commonwealth offence. Relevant subsection 16A(2) factors include:

    …

    (d) the personal circumstances of any victim of the offence;

    (e) any injury loss or damage resulting from the offence; and

    (ea) if an individual who is a victim of the offence has suffered harm as a result of the offence – any victim impact statement;

39. Any harm which is occasioned to a victim as a result of the offending is already a relevant factor when considering the appropriate sentence to impose. However, the Law Council is concerned that, were an aggravated offence created which was predicated on a causal link to harm to a victim, such an offence would be unduly difficult to prove and would likely result in greater trauma for the victim of the offence.

40. To prove an aggravated offence, the prosecution would need to establish beyond reasonable doubt that the harm occasioned to the victim (whatever that may be) was caused by the actions of the offender. This would seem difficult to prove to the relevant standard and would necessarily require a victim (if available) to give evidence as to the harm they suffered and be cross-examined as to the causation of that harm. In circumstances where a victim self-harmed as a result of bullying, this would undoubtedly be a difficult, and perhaps traumatic experience.

41. Alternatively, where the prosecution alleges that a victim has suffered harm relying on subsection 16A(2) factors, where such harm is not an element of the offence, the fact need only be proved for example in Queensland on the balance of probabilities (appropriately adjusted on a sliding scale for the gravity of the allegation). In many cases, submissions regarding the level of harm caused to a victim may be able to be agreed between the parties on sentence, without the need to prove a formal

[35] The Law Council acknowledges the input from the Bar Association of Queensland for drawing many of the issues in this section to the Law Council's attention.

circumstance of aggravation. Further, if harm to a victim were legislated as a formal circumstance of aggravation, the prosecution would lose the ability to allege any harm to a victim without formally charging that circumstance and proving it to the requisite standard. Adding a formal circumstance of aggravation would see victims heard less in sentencing proceedings as prosecuting authorities would be cautious about bringing aggravated charges (where strict proof is required) where they would have otherwise been able to rely on a victim impact statement to show harm for the offence as it currently stands.

42. In the view of the Law Council, if it is thought that the penalties for section 474.17 offences are not meeting community expectations, not appropriately addressing the impact to victims or not presenting and adequate deterrent in light of increased prevalence, the best way forward to increase, generally, the maximum penalty applicable for a section 474.17 offence.

43. The offence currently carries a maximum penalty of 3 years imprisonment. More 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.

44. In summary, the Law Council would not oppose a general increase to the maximum penalty for a section 474.17 offence, provided it did not go beyond a maximum of 5 years imprisonment.

45. However, the Law Council opposes any move to introduce an aggravated offence which is contingent upon harm to the victim. The Law Council believes that the Crimes Act already provides adequate scope for the harm to a victim to be considered in the sentence imposed. The most appropriate sentencing outcomes will be achieved by a Judge or Magistrate weighing up all of the relevant section 16A considerations, including the harm to a victim.

Recommendations:

- **An aggravated cyberbullying offence which is contingent upon harm to the victim should not be introduced.**
- **The Committee consider whether a maximum of 5 years imprisonment for a section 474.17 Criminal Code offence would be appropriate.**

Minimum standards for sentencing young cyberbullying offenders

46. The Law Council supports effective minimum standards for the sentencing of young offenders who may be perpetrators of cyberbullying. Some important concerns about the operation of current sentencing laws with respect to young offenders were identified by the ALRC as part of its 2006 *Same Time, Same Crime: Sentencing of*

Federal Offenders report.[36] The ALRC proposed a number of important changes in this regard, including that:

(a) federal sentencing legislation should establish minimum standards for the sentencing, administration and release of young federal offenders; and

(b) when sentencing a young federal offender, the court should be required to have regard to: the young person's wellbeing; and the requirement that children be detained only as a measure of last resort, and only for the shortest appropriate period.[37]

47. As yet, there has been no Australian Government response to this report. The Law Council would support such a response and, in particular, supports the above recommendations made by the ALRC.

48. In the current context, several other aspects of the Crimes Act are worth noting in respect of concerns about the sentencing of minors. These include that:

(a) the court must impose a sentence or make an order that is of a severity appropriate in all the circumstances of the offence.[38] The matters that the court must take into account in reaching this decision include the age of the person;[39]

(b) where a period of imprisonment only is specified as the maximum penalty, a fine may nevertheless be imposed;[40] and

(c) a child or young person who, in a state or territory, is charged with or convicted of an offence against a law of the Commonwealth may be tried, punished or otherwise dealt with as if the offence were an offence against a law of the state or territory.[41] This enables young federal offenders to be dealt with by the specialist juvenile justice systems which are established in the states and territories. In particular, judges would be able to utilise state and territory alternative sentencing options for young offenders, which may include community service orders and other diversionary options. It is noted, however, that the available options will vary depending upon the jurisdiction involved.

Recommendation:

- **The recommendations of the ALRC which emphasise the need for federal sentencing legislation to establish minimum standards for the sentencing of young offenders should be adopted to enhance sentencing practices for young cyberbullying offenders.**

[36] Australian Law Reform Commission, *Same Crime, Same Time: Sentencing of Federal Offenders report*, ALRC Report 103 (tabled 13 September 2006), Chapter 27 (Young Federal Offenders).
[37] Ibid, recommendation 27-1.
[38] *Crimes Act 1914* (Cth) s 16A(1).
[39] *Crimes Act 1914* (Cth) s 16A(2)(m).
[40] *Crimes Act 1914* (Cth) ss 4B(2) and 4B(2A).
[41] *Crimes Act 1914* (Cth) s 20C.

The adequacy of the policies, procedures and practices of social media platforms in preventing and addressing cyberbullying

Best practice response

49. Research from UK anti-bullying charity Ditch the Label found in July 2017 that, of those that reported being cyberbullied, 42% experienced cyberbullying on Instagram, 37% on Facebook, 31% on Snapchat and 9% on Twitter.[42]

50. Under the *Enhancing Online Safety Act 2005* (Cth) (**Enhancing Online Safety Act**) social media service 'tier scheme' under the, Facebook, Instagram, YouTube and Google+ are currently listed as a tier 2 services, and airG, Ask.fm, Flickr, Snapchat, Twitter, Yahoo!7 Answers and Yahoo!7 Groups are listed as tier 1 services.

51. As discussed below, tier 2 services may be liable to a civil penalty, but not tier 1 services.

52. Research shows that most of these social media platforms have internal policies and procedures, and online practices to prevent and address cyberbullying, including help centres, 'bullying prevention hubs,' and teams fielding reports of inappropriate content.[43]

53. The 'Statement of Rights and Responsibilities' (**SRR**) constitutes the terms of service that govern the relationship between Facebook users, others who interact with Facebook, and Facebook brands, products and services.[44] This includes a commitment by users that they will 'not bully, intimidate or harass any user'.[45]

54. There are a number of issues with the operation of the SRR:[46]

    (a) The Facebook SRR indicates that it is subject to the law of the United States.[47] This may lead to conflict of law issues, meaning Australian legislative provisions may not be enforceable. However, in France in 2012, a judge found that French law was applicable in a dispute where Facebook was a party.[48]

---

[42] Ditch the Label, *The Annual Cyberbullying Survey 2017* (July 2017) available at https://www.ditchthelabel.org/wp-content/uploads/2017/07/The-Annual-Bullying-Survey-2017-1.pdf.
[43] Sarah Kessler, 'How Facebook Handles Inappropriate content' (2012) <http://mashable.com/2012/06/19/facebook-inappropriate-content/#TtTUjeWgZEqJ>.
[44] Facebook, *Statement of Rights and Responsibilities,* available at https://www.facebook.com/legal/terms.
[45] Ibid.
[46] See Eva Lievens, 'Bullying and sexting in social networks: protecting minors from criminal acts or empowering minors to cope with risky behaviour' (2014) 42 *International Journal of Law, Crime and Justice* 251, p. 263.
[47] Facebook, *Statement of Rights and Responsibilities,* available at https://www.facebook.com/legal/terms: "You will resolve any claim, cause of action or dispute (claim) you have with us arising out of or relating to this Statement or Facebook exclusively in the U.S. District Court for the Northern District of California or a state court located in San Mateo County, and you agree to submit to the personal jurisdiction of such courts for the purpose of litigating all such claims. The laws of the State of California will govern this Statement, as well as any claim that might arise between you and us, without regard to conflict of law provisions.'
[48] Court of Appeal of Pau, First Chamber, Judgment of 23 March 2012, <http://www.legalis.net/spip.php?page¼brevesarticle&id_article¼3382> [in French] citied in Eva Lievens, 'Bullying and sexting in social networks: protecting minors from criminal acts or empowering minors to cope with risky behaviour' (2014) 42 *International Journal of Law, Crime and Justice* 251, p. 263.

(b) Whether an Australian minor is capable of agreeing to the SRR, and therefore whether the SRR is legally binding.[49] Even if a minor can legally enter into the agreement, there may be issues as to whether the minor knows and understands of the content of the SRR, as the terms are lengthy, involve complex language, and are easy to agree to without reading the full text.

(c) Under the SRR, Facebook denies any liability for content or behaviour of users.[50] It is uncertain whether there are some circumstances that would make this term invalid.

(d) When content has been reported to Facebook, they are not legally required to remove the content. Facebook has discretion to remove content that violates local laws but not the Community Standards. Where this occurs, they will review the content to determine if it is illegal under local law, and then 'may make it unavailable only in the relevant country or territory'.[51]

55. Considering the legal challenges around enforcement, and getting social media sites to remove harmful content, the Law Council believes the Australian Government should continue to work with social media sites to develop a best practice in response to cyberbullying.

56. For example, in the European Union (**EU**), two separate Coalitions consisting of social media companies, and with the support of the EU Commissioner, have been formed to continue working towards effective ways to combat cyberbullying experienced by children.[52]

Panic buttons

57. One practical and inexpensive suggestion is for social media platforms to provide a panic button which a young person can click to report online abuse or any inappropriate or potentially illegal activity directly to appropriate authorities. The advantage of having such a panic button is that victims do not have to contact the police which can often be intimidating, time consuming and ineffective. Instead, the panic button provides them the opportunity to report any act of cyberbullying in a timely manner to authorities skilled in dealing with such incidents.

58. This has in fact already occurred in the United Kingdom: after receiving a significant number of complaints about Facebook in early 2010, Facebook authorities installed a panic button on its home page for UK-based Facebook members. Facebook members from UK between the age of 13 and 18 years can install the panic button application

---

[49] Eva Lievens, 'Bullying and sexting in social networks: protecting minors from criminal acts or empowering minors to cope with risky behaviour' (2014) 42 *International Journal of Law, Crime and Justice* 251, p. 263.
[50] Facebook, *Statement of Rights and Responsibilities,* available at https://www.facebook.com/legal/terms: 'If anyone brings a claim against us related to your actions, content or information on Facebook, you will indemnify and hold us harmless from and against all damages, losses, and expenses of any kind (including reasonable legal fees and costs) related to such claim. Although we provide rules for user conduct, we do not control or direct users' actions on Facebook and are not responsible for the content or information users transmit or share on Facebook. We are not responsible for any offensive, inappropriate, obscene, unlawful or otherwise objectionable content or information you may encounter on Facebook. We are not responsible for the conduct, whether online or offline, of any user of Facebook'.
[51] Facebook, *Community Standards,* <https://www.facebook.com/communitystandards>.
[52] The Coalition to Make the Internet a Better Place for Kids and the ICT Coalition for the Safer Use of Connected Devices and Online Services by Children and Young People in the EU.

and report cyberbullying to appropriate authorities. Facebook has not provided such an application to its users in Australia.[53]

59. However, installing a panic button or any other form of alarm/reporting tool on a social networking site has limited benefits. What is required is that authorities inform young users and their parents the benefits of the tool. The main limitation of such an alarm tool is that only the victims have the ability to lodge a complaint of the offensive content; parents or guardians are unable to take such actions on their behalf. Parents or guardians should be afforded the opportunity to take actions to protect their child from harm.[54]

The role of parental supervision

60. Due to the difficulties encountered by parents and guardians in supervising their child's online activity, concerns have been raised about their ability to intervene when their child is being cyberbullied. If their child has been the target of cyberbullying, parents, guardians or a responsible adult who has the consent of the child may lodge a complaint to the eSafety Commissioner.[55] The ability for parents or guardians to intervene where their child is the target of cyberbullying could be strengthened by social media sites making any complaint lodged by a parent or guardian being high priority for the site.[56]

Recommendation:

- **The Australian Government should continue to work with social media sites to develop a best practice in response to cyberbullying. The Australian Government should continue to work with social media sites to develop a best practice in response to cyberbullying. This may include for example prioritisation of a parent's/guardian's complaint in relation to cyberbullying content.**

Other measures used to combat cyberbullying between school children and young people

61. A key issue is the awareness and training of the Australian Police Force about the various laws that may be applicable to incidents of cyberbullying.[57] 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.[58]

62. There may be value, therefore, for increased education and awareness of the possible consequences of cyberbullying, for law enforcement, prosecutors and the judiciary.

63. A critical measure designed to combat cyberbullying between school children and young people was the establishment of the eSafety Commissioner by the Enhancing

[53] Aashish Srivastava, Roger Gamble and Janice Boey's, 'Cyberbullying in Australia: Clarifying the Problem, Considering the Solutions' (2013) 21 *International Journal of Children's Rights* 25, p. 37.
[54] Ibid.
[55] *Enhancing Online Safety Act 2015* (Cth) s 18.
[56] Aashish Srivastava, Roger Gamble and Janice Boey's, 'Cyberbullying in Australia: Clarifying the Problem, Considering the Solutions' (2013) 21 *International Journal of Children's Rights* 25, p. 38.
[57] Ibid.
[58] Ibid, p. 41.

Online Safety Act, which has the power to investigate complaints and also remove content from the internet.

64. The Law Council also considers that more could be done to increase the profile and awareness of the Office of the eSafety Commissioner and the action it can take in relation to cyberbullying.

65. In addition, the Law Council recognises the work of the Office of the eSafety Commissioner delivering online safety education to schools. As part of this program, the Law Council recommends that educational measures seek to make the public aware that the most serious instances of cyberbullying may constitute criminal conduct under existing Commonwealth legislation. Such messages should explain the application of these offences, and the relevant terminology, in a clear and accessible manner.

Recommendation:

- **The Australian Government should consider increased education and awareness of the possible consequences of cyberbullying, including criminal prosecution under the existing offences, for the community, law enforcement, prosecutors and the judiciary. Such messages should explain the application of these offences, and the relevant terminology, in a clear, accessible manner.**

Investigative powers of the eSafety Commissioner

66. The eSafety Commissioner currently has powers to investigate complaints made by a child, their parent or guardian, or a responsible person who has the consent of the child.[59] The eSafety Commissioner may investigate the complaint 'as the Commissioner sees fit'.[60] In considering the complaint, the eSafety Commissioner may require evidence in the form of a receipt or complaint number issued by the social media service, or where this is not available a screenshot, statutory declaration or 'such other form as the Commissioner specifies'.[61]

Removal of content provisions

67. There is a difference under the Enhancing Online Safety Act between the way in which the eSafety Commissioner treats 'tier 1' and 'tier 2' services. Tier 1 services are requested by the eSafety Commissioner to remove material on a voluntary basis and tier 2 services may be subject to a civil penalty regime. The distinction gives 'tier 1' services a chance to take the harmful content voluntarily without being subject to enforcement mechanisms straightaway.

68. Following the eSafety Commissioner receiving a complaint of cyberbullying material, they may request that a tier 1 social media service remove material.[62] If the eSafety Commissioner is satisfied the material breaches provisions which prohibit end-users from posting cyberbullying material, and a complaint was lodged to the service and not removed within 48 hours, the eSafety Commissioner may give the provider of the service written notice requesting them to remove the material within 48 hours.[63]

---

[59] *Enhancing Online Safety Act 2015* (Cth) ss 18-19.
[60] Ibid, s 19(2).
[61] Ibid, s 18(7)-(8).
[62] Ibid s 29.
[63] Ibid s 29.

However, there are no enforcement mechanisms if the social media service fails to do so.

69. Tier 1 social media services will be downgraded to tier 2 services if they do not comply with the eSafety Commissioner's request to take down material. Revocation of a tier 1 declaration of social media service requires at least 12 months to have passed since the declaration was made and that, during that time, the provider has repeatedly failed to comply with written notice requests given to the provider to remove material.[64] This is a long period in which serious consequences could occur from cyberbullying. The Act does not appear to provide for any discretionary provisions enabling the eSafety Commissioner to revoke the tier 1 status if the provider has clearly failed to remove material with potentially serious consequences. This may undermine the object of the Enhancing Online Safety Act to ensure that harmful material is removed quickly.

70. For a social media service to be declared as a tier 1 service, it must satisfy the eSafety Commissioner that it complies with 'basic online safety requirements'.[65] These requirements have a very low threshold. For example, the social media service's terms of use must contain a provision that prohibits end-users from posting cyberbullying material on the service, the service must have a complaints scheme under which end-users can request the removal of cyberbullying, and there must be an individual who is designated as the service's contact person.[66]

71. The 'basic online safety requirements' do not include other safeguards which would promote online safety, such as record keeping about complaints and their handling or timeframes for responding to complaints to ensure a prompt response.

72. Tier 2 providers have to be declared by the eSafety Commissioner who can enforce requests for removal if a tier 2 provider fails to comply with them.[67]

73. Where a tier 2 social media service fails to remove cyberbullying material within 48 hours of a complaint being made to the service's complaints scheme, the Commissioner may give the social media service a notice.[68] If the social media service does not comply with the notice they may be liable to a civil penalty of 100 penalty units.[69]

74. The tier 2 enforcement scheme applies only to 'large social media services,' not to small providers.[70] The characterisation of a 'large social media service' is unclear and is subject to the eSafety Commissioner's discretion, having regard to certain factors. In addition, the Law Council questions whether small providers should also be captured to permit the eSafety Commissioner to enforce requests.

Recommendations:

- **The distinction between tier 1 and tier 2 social media services in the *Enhancing Online Safety Act 2005* (Cth) should be maintained. However, the 12 month period in which a non-compliant tier 1 service is downgraded to a tier 2 service may be too long and may lead to serious consequences occurring from cyberbullying. The Law Council recommends that the eSafety Commissioner be given a discretion to**

[64] Ibid s 25.
[65] Ibid s 23(4)(b).
[66] Ibid s 21.
[67] Ibid ss 30-31.
[68] Ibid s 35.
[69] Ibid s 36.
[70] Ibid s 31.

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.

- **The tier 2 enforcement scheme should be expanded to permit the Commissioner to enforce requests for removal of content from small service providers.**

Availability of a range of penalties

75. In the absence of a new federal offence being created, the Law Council continues to support a strengthened civil penalty regime to target cyberbullying, noting that there are several considerations that should be addressed to ensure an effective regime, such as resourcing for the provision of counselling and other support for affected individuals.[71]

76. Where the perpetrator, complainant and other individuals are children, the Law Council notes that other responses by the eSafety Commissioner may be appropriate as initial steps prior to the mechanisms above, including mediation and negotiation. For example, it has been suggested to the Law Council that conferencing which draws on restorative justice principles, may be appropriate in certain circumstances. This would provide an opportunity for: (a) the affected child to explain the harm that has been done, and the consequences of that harm; (b) the offender to acknowledge the harm, and to apologise for his or conduct, as well as to commit to specific undertakings as reparation.

77. A range of penalties may apply if social media sites or individuals fail to comply with the eSafety Commissioner's notices. For individuals, this may include:

    (a) publishing statements about non-compliance with notices to remove material;[72]

    (b) issuing formal warnings;[73] and

    (c) issuing infringement notices to social media services, which may include an appropriate fine.[74]

78. Careful consideration will need to be given to circumstances under which the eSafety Commissioner might serve an infringement notice to an individual under 18 years old.

79. Given the variety of conduct which will need to be investigated by the eSafety Commissioner, the Law Council recognises that the eSafety Commissioner needs to have a broad range of tools at his or her disposal to appropriately respond to the

---

[71] Law Council of Australia, Enhancing Online Safety for Children Inquiry, *Submission to the Department of Communications* (7 March 2013) <https://www.google.com.au/search?dcr=0&source=hp&q=enhancing+online+safety+for+children+inquiry+%E2%80%93+submission+to+the+department+of+communications+7+march+2014&oq=enhancing+o&gs_l=psy-ab.3.0.35i39k1l2j0l8.1803.8304.0.9512.12.9.0.0.0.0.286.977.0j1j3.4.0....0...1.1.64.psy-ab..8.4.976.0..0i67k1j0i131k1.0.oQluHz6kOak> p. 5.
[72] *Enhancing Online Safety Act 2015* (Cth) ss 39-40.
[73] *Enhancing Online Safety Act 2015* (Cth) ss 37, 44
[74] *Enhancing Online Safety Act 2015* (Cth) s 36.

circumstances of any particular complaint. In the gravest cases, the eSafety Commissioner will need to refer possible criminal conduct to the police.

80. However, the Law Council considers that, in deciding the most appropriate enforcement mechanisms in situations where the perpetrator is a child, the eSafety Commissioner should have regard to the: (a) best interests of the child; and (b) need to promote the likelihood that the child will reintegrate and assume a constructive role in society.

Recommendations:

- **The eSafety Commissioner should be adequately resourced to effectively implement the existing civil penalty regime to target cyberbullying and other considerations such as the provision of counselling and other support for affected individuals.**
- **The eSafety Commissioner should be provided with greater flexibility regarding the range of appropriate penalties, enforcement mechanisms and other responses to deal with cyberbullying in the most appropriate manner.**