AFP
AUSTRALIAN FEDERAL POLICE

Department of Communications

Enhancing Online Safety for Children Discussion Paper

Submission by the Australian Federal Police

March 2014

Introduction

The AFP welcomes the opportunity to make a submission in response to the Department of Communications' Discussion Paper, *Enhancing Online safety for Children*.

2. The AFP strongly supports initiatives to enhance online safety for children. The use of technology, particularly the Internet and social media, is increasingly becoming a significant part of the lives of young persons. Technology is a great tool to easily and rapidly access information and allows peer-to-peer interaction. However, online interactions can expose children to exploitation and unsolicited communications and behaviours (including bullying and harassment). The AFP recognises the significant and sometimes devastating impact that cyber-bullying can have on young people's lives.

3. Prevention is one of the key pillars of modern day policing and the AFP is dedicated to preventing all Australians from becoming victims of cybercrime by empowering them to use technology safely and responsibly. The AFP has a significant role to play in ensuring children and young people are safe, no matter what environment they are in. In fulfilling this role, the AFP has forged strong partnerships with all Australian law enforcement agencies, many international agencies, government departments, industry and not-for-profit organisations.

4. The AFP is involved in many crime prevention and awareness raising initiatives, particularly in relation to keeping young people safe online. The *ThinkUKnow* Australia website is a partnership between the AFP, industry and some State and Territory police services, and aims to raise awareness among parents, carers and teachers of the issues that young people face online. That is to say, educating those responsible for the care and custody of children by bridging the knowledge gap between adults and children.

5. The *ThinkUKnow* website provides information on technologies and applications young people use to have fun online, the risks they face and how to stay in control, and how to report when things go wrong. There are specific "report buttons" for inappropriate sexual behaviour towards children online, prohibited or inappropriate Internet content and spam. The *ThinkUKnow* cybercrime prevention program was developed in the United Kingdom (UK). The AFP was granted an exclusive license by the UK Child Exploitation Online Protection (CEOP) Centre to implement *ThinkUKnow* in Australia.

Response to Discussion Paper

6. The Discussion Paper canvasses a range of issues relevant to: the proposed establishment of a Children's e-Safety Commissioner; a mechanism to ensure material that is harmful to a child is rapidly removed from social media sites (rapid removal mechanism); and options for dealing with cyber-bullying under Commonwealth legislation. This submission focusses on three specific aspects of the Discussion Paper:

- the existing programs for which the proposed Commissioner would be responsible for;
- enforcement challenges; and
- criminalisation of cyber-bullying.

Children's e-Safety Commissioner

7. The AFP supports the establishment of the Commissioner as an accessible and centralised point of contact to address online safety for young people. The Commissioner could assist in promoting and improving the safety of Australian children online — a mandate the AFP strongly supports. By taking a proactive and educative focus, the Commissioner could actively work to reduce harassment and bullying, and provide appropriate support services to young people. As part of this educative role, the Commissioner could clarify how current Commonwealth, State and Territory criminal law apply to cyber-bullying behaviour.

8. The AFP acknowledges the broad benefits of transferring some existing e-Safety programs to the proposed Commissioner's control. The Discussion Paper notes that programs aimed at improving the online safety of people of all ages may not be suitable for transfer to the Commissioner (whose focus would be child safety) and that there are benefits of the AFP *ThinkUKnow* program (including the "report button" function) remaining with a law enforcement body.

9. There are significant benefits to the AFP continuing to administer the *ThinkUKnow* program rather than transferring it to the proposed Commissioner. Firstly, the focus of *ThinkUKnow* is on raising adult awareness of cyber safety. Secondly, the program harmonises law enforcement messaging on cyber safety with most Australian law enforcement agencies having either joined the *ThinkUKnow* partnership or are drafting Memoranda of Understandings to become partners.

10. Thirdly, as discussed above, the *ThinkUKnow* website also provides a mechanism for reporting online sexual abuse of children. This capability is a result of the AFP's membership of the Virtual Global Taskforce (VGT). The VGT is an international partnership of law enforcement agencies committed to combating online child sexual abuse worldwide. Allegations made through the

"report button" are received directly by the AFP's Child Protection Operations Team, assessed, triaged and where appropriate directed to the relevant State or Territory. Given the nature of the reports received, it is essential that this particular function of the *ThinkUKnow* website remains with a law enforcement body.

11. The AFP does, of course, support working with the Commissioner to enhance online safety for children. The Commissioner could be kept informed of the delivery and initiatives of *ThinkUKnow*, and where appropriate be involved in the program.

Enforcement challenges

12. In the context of the proposed rapid removal mechanism, the Discussion Paper acknowledges enforcement challenges where the content is hosted in another country, and/or where the content host has a limited corporate presence in Australia. The AFP notes that these enforcement challenges would also occur should a civil penalty and infringement notice scheme be introduced. In this regard, the AFP recognises the very good relationship it has with domestic and international industry partners who operate in the online environment. The AFP relies on the voluntary cooperation of international companies in support of law enforcement operations.

13. The AFP supports relying on section 474.17 to address cyber-bullying (the rationale for this is discussed in the next section), however acknowledges the difficulties in gathering admissible evidence located in overseas jurisdictions.

Criminalisation of cyber-bullying

14. The Discussion Paper discusses possible options for dealing with cyber-bullying under Commonwealth legislation, including new criminal offences and/or a civil penalty and infringement notice regime.

15. The AFP considers that section 474.17 of the *Criminal Code* is more than adequate to facilitate prosecution of cyber-bullying cases where appropriate. Rather than being 'too general', the AFP considers that the breadth of section 474.17 is its strength, capturing a wide range of behaviours in a rapidly evolving online environment.

16. The AFP is not aware of any operational deficiencies in section 474.17 that need to be addressed that would justify creating a new, specific Commonwealth cyber-bullying offence.

17. The Discussion Paper suggests that a specific cyber-bullying offence may be appropriate so that a lower maximum penalty could be applied. While the offence in section 474.17 carries a maximum penalty of three years imprisonment, it will be open to the court to impose a sentence that is proportionate to the circumstances of each case in accordance with common law and statutory sentencing principles. Should a particular instance of cyber-bullying be considered to fall on the lower end of the spectrum of offending, the court would be able to impose a penalty falling well below the maximum of three years imprisonment.

18. There are also general provisions in the *Crimes Act 1914* (Cth) which could apply to offences under section 474.17, allowing for lower penalties and/or penalties other than imprisonment to be applied. Section 4B provides that, unless the contrary intention appears, the court may (if appropriate in the circumstances of the case) impose a pecuniary penalty instead of imprisonment. Under section 4J, a section 474.17 offence could be dealt with summarily, and as a consequence the maximum penalty that could be imposed is 12 months imprisonment and/or a fine of up to 60 penalty units. Further, when sentencing an offender under 18, a court is able to access alternative sentencing options that are available under State/Territory law, such as a fine or a good behaviour bond (for example, see section 33 of the *Children (Criminal Proceedings) Act 1987* (NSW)).

19. The Discussion Paper notes concerns that many minors are not aware of the existence, and potential application, of section 474.17. However, the AFP does not consider that this factor in and of itself warrants any changes to Commonwealth legislation. Further, creating a new, specific cyber-bulling offence could lead to confusion about the application of the existing offence. The AFP considers that a more effective mechanism would be, for example, the proposed Commissioner raising awareness and educating youth about how the offence could apply to their behaviour online.

20. The AFP considers that there may be merit in further exploring how a civil penalty and infringement notice scheme could be administered by the proposed Commissioner. On the face of it, the proposed scheme could provide a more expedient process for dealing with the majority of cyber-bullying cases, allowing police to focus their resources on investigating the most serious cases of cyber-bullying. However, if the proposed scheme proceeds, it will be important to clarify how it will interact with existing State and Territory action to mediate and address cyber-bullying allegations. Further, careful consideration will need to be given to how the Commissioner's Office would be resourced to develop the necessary capability to pursue civil enforcement action, particularly where evidence of contraventions by overseas-based social media sites is involved.