The Director, Cyber Safety Policy and Programs

Department of Communications

GPO Box 2154

Canberra ACT 2601

February 14, 2014.

Comments relating to public consultation paper *Enhancing Online Safety for Children*

Dr Colette Langos (BA, LLB, GDLP, MCom Law, PhD)[1]

I commend the Australian Government for committing to improving the online safety of children in Australia. I hereby provide brief comments for consideration by the Department of Communications relating predominantly to *Part 3* the public consultation paper *Enhancing Online Safety for Children* (2014).

As a prelude to my comments, it necessary to highlight just how complex the phenomenon cyberbullying is.

[1]Member of the South Australian Law Society and Member of the Children and the Law Committee, Law Society of South Australia; Lecturer at the University of South Australia, School of Law. (Note, the opinions expressed below are the opinions of the *author* and do not necessarily reflect the views of the other members of the Law Society of South Australia Children and the Law Committee).

Contact Details: Dr Colette Langos, School of Law, University of South Australia. GPO Box 2471, Adelaide, South Australia 5001. Colette.Langos@unisa.edu.au.

There is no universal definition of 'cyberbullying' and it is not presently defined in any Australian state or territory legislation. There is, however, general consensus that cyberbullying involves intentional and aggressive (malicious) conduct facilitated through information communication technologies (ICTs) (Langos, 2013a; Langos, 2012). It relates to online conduct intended to harm another. In a cyberbullying context, 'harm' includes emotional harm, which includes a very broad range of negative emotional feelings including anxiety, annoyance, grief, fear and humiliation as well as more severe psychological harm; protracted psychological injury. Cyberbullying occurs in multiples context and can be direct or indirect. Direct cyberbullying occurs where the cyberbully directs the electronic communications to the victim only (as opposed to communications which are posted to publically accessible areas of cyberspace) (Langos, 2012). It occurs in the private online domain. Indirect cyberbullying occurs in instances where the electronic communication is not sent directly to the victim (Langos, 2012). Instead, the cyberbully posts the communication to a publically accessible area of cyberspace. Public forums such as social media sites, publically accessible blogs and websites and video sharing websites are obvious examples of platforms which fall within the public online domain. The concept of the public online domain extends to situations where there are multiple recipients of an electronic communication, given the lack of control over the material once it is sent to multiple parties (Langos, 2013b). The communication has the potential to spread like 'wildfire' given that any of the recipients could forward, save and repost the material at a later stage. The reach of the material is in this manner uncontained and lies outside the parameters of the private online domain.

The consultation paper does not make reference to the various different forms of cyberbullying discussed in the literature to date. Manifestations include: ‘harassment’; ‘cyberstalking’; ‘denigration’; ‘happy slapping’; ‘exclusion’; ‘outing and trickery’; ‘impersonation’ or ‘masquerading’; and ‘indirect threat’ (Langos 2013a; Langos, 2013b). Not all forms of cyberbullying are equally harmful. There are many ‘shades of harm’ associated with cyberbullying. Some victims may experience negligible (Ybarra et al, 2006) or mere trivial harm and others may experience protracted psychological injury (Langos, 2013b, 117-126). It is exceedingly difficult to generalize the extent of harm associated with each particular form of cyberbullying. Langos (2013b) has assessed the level of harm associated with each particular form based upon the degree to which a victim’s individual interests (physical integrity; freedom from humiliation; privacy/autonomy) are impeded in typical instances. Drawing upon existing findings and a theoretical model, it is possible to posit that some forms are inherently more harmful than others and rank the various manifestations of cyberbullying from most serious to least serious (Langos, 2013b). Given the infancy of cyberbullying research, a state ought to act cautiously when considering intervening by way of the criminal law. A state may be justified in criminalizing some forms of cyberbullying and not others based on the potential harmfulness of the conduct. Policy makers ought to be mindful of this should the option of creating a separate cyberbullying offence be pursued.

What is uncontentious from initial findings is that, at the very least, a degree of danger is involved for individuals exposed to cyberbullying. Early findings demonstrate that cyberbullying is associated with a range of negative implications such as high levels of anxiety (Juvonen and Gross, 2008), suicidal ideation (Hinduja and Patchin, 2010), depression (Wang, Nansel and Iannotti, 2011), psychosomatic problems (Sourander et al., 2010), as well

as behavioural problems, such as aggressive behaviours and excessive consumption of alcohol (Sourander et al, 2010). Such consequences are similar to those reflected in traditional (without the use of information communication technologies) bullying research (Rigby, 2003). The wave of cyberbullying-related suicides both in Australia and overseas continues to intensify community concern (see, for example, Chloe's Law movement, part of which is an online community of 287,000 Australians advocating for heavier penalties for bullying and cyberbullying; federal Chole's Law petition to the Australian senate (sponsored by Senator Eric Abetz 2013-2014); Tasmanian Chloe's Law petition to the Tasmanian House of Assembly (sponsored by Jacquie Pertrusma MP and Shadow Attorney-General Vanessa Goodwin MP 2013)). Notably, various Australian publications have reported cyberbullying as an emerging risk factor associated with Australian youth suicide (for example, Commission for Children and Young People and Child Guardian, 2012; Commonwealth Government, 2011). Importantly, recent studies have shown that victims of cyberbullying experience *more severe* mental health implications than victims of traditional bullying (Campbell et al., 2012; Perren et al., 2010). Early findings thus suggest that cyberbullying is a more sinister species of bullying.

Overseas jurisdictions (for example, New Zealand, United States, Canada, United Kingdom, Germany), like Australia, are grappling with the legal regulation of the phenomenon. Legal regulation in isolation is unlikely to curb the behaviour. A *multifaceted response* is required to manage this (potentially devastating) behaviour in a holistic manner. It is imperative that any legal initiatives are complemented by, for example, those school-based intervention strategies research informs as being the most effective; ensuring restorative justice practices are implemented as part of school and workplace conflict resolution mechanisms for managing instances of cyberbullying and other relationship problems; raising awareness

as to how to identify cyberbullying; educating adults and children as to how they can best respond when exposed; and raising awareness in relation to the criminal laws which prohibit instances of cyberbullying.

I am in support of those initiatives discussed in *Parts 1 and 2* of the consultation paper. Establishing a Children's e-Safety Commissioner will provide a clear central contact point for targeted Australian youths. The functions listed in the proposal complement existing federal government initiatives and appear appropriate.

I am also in support of the scheme enabling the rapid removal of harmful material from large social media sites. It is exceedingly difficult to strike the right balance between a young person's right to freedom of expression/speech and their right to develop (physically and mentally) in conditions of freedom and dignity. Policy makers need to be mindful not to define harmful content in an overly broad manner when defining what sort of material is 'harmful' enough to justify its removal.

Alongside non-criminal measures, Australian states and territories would be prudent to review their criminal laws to ensure that the most serious manifestations of cyberbullying are adequately regulated at the state level. There is an argument to be made that states ought to enact a separate specific cyberbullying offence, notwithstanding any federal legislative initiatives (Langos, 2013b). In instances where both state and Commonwealth legislation governs, it is often a matter of who 'gets there first' that will determine whether the matter is handled by the state or the Commonwealth. However, state police are, generally speaking, more assessable to the general public. Thus, where a matter can be prosecuted under both state and Commonwealth legislation, more times than not, a matter will be pursued by state police under state legislation. Where no state legislation governs

the alleged conduct, the Commonwealth is most likely to prosecute where a Commonwealth interest is at stake (e.g. the victim is a Commonwealth employee) or in cases where the alleged conduct is of a serious nature given the severity of the existing penalty for s 474.17 and limited federal resources.

The following comments relate specifically to *Part 3* of the public consultation paper which discusses options for dealing with cyberbullying under *federal* legislation.

Specifically, Q20:

In light of the Government's proposed initiatives targeting cyberbullying set out in Chapters 1 and 2; do the current criminal laws relating to cyberbullying require amendment?

I support amending section 474.17 of the *Criminal Code*.

This offence is a broad misuse of telecommunications provision. It does not require conduct to occur more than once and does not require proof of an intention to harm, proof of harm, or require a victim. The reach of the provision is thus not limited to regulating instances of cyberbullying (cyberbullying necessarily requires an intention to harm and a victim). Section 474.17 of the *Criminal Code* regulates a broad range of generally aggressive online conduct including cyberbullying.

All cyberbullying involves 'use of a carriage service' to facilitate the online conduct. Cyberbullying instances may involve 'menacing' conduct. This could occur in instances where a perpetrator threatens a victim with physical harm. This may also occur in instances

where a victim is threatened with harm to a business or personal reputation. Equally, cyberbullying could involve 'harassing' conduct. Additionally, it is conceivable that every form of cyberbullying could be considered 'offensive'. However, only those instances of cyberbullying that a *reasonable* person would consider to be 'menacing, harassing, or offensive', fall within the scope of the offence. Thus, it is likely that short-term 'exclusion' and isolated instances of 'denigration' would not be regulated by section 474.17. Such forms are considered 'bottom-end' cyberbullying, likely to cause a victim only marginal or negligible harm. On the other hand, instances of 'denigration', 'masquerading' or 'impersonation', 'outing' and 'trickery', 'exclusion' or 'happy slapping' could be governed by this provision (Langos, 2013b).

Although highly applicable to instances of both direct and indirect cyberbullying, in its current form, the way the provision is worded does not make it obvious to youths, or the public generally, that s 474.17 prohibits cyberbullying. It is highly likely that youths would not realise that the terms 'use of a carriage service' relates to, for example, sending SMS messages or using the Internet. By amending the language of this offence more Australians are likely to realize that sending menacing, threatening or offence material via, for example, SMS messages or the Internet, is prohibited. Policy makers may consider it appropriate to incorporate a cyberbullying definition in an amended version/iteration of section 474.17. This would provide much needed clarity as to definition of the behaviour.

Q21 ***Is the penalty set out in section 474.17 of the Criminal Code appropriate for addressing cyberbullying offences?***

The existing maximum penalty associated with a section 474.17 offence is a term of imprisonment of up to three years and/or a fine of up to $30,600. This is a relatively serious offence. The consultation paper reports that there have been 308 successful prosecutions under this offence over the past 9 years, 8 of those involving persons under the age of 18 years. It is highly likely that the 8 youths were prosecuted for *very* serious instances (inherent nature of the conduct and or the repetitive nature of the conduct) of cyberbullying. Most instances of cyberbullying involving young people are resolved either within the school context via school disciplinary measures and conflict resolution mechanisms; via discussions with police (issuing of warnings); diversionary options. It may be appropriate to make a special provision in the legislation, in the form of a lower maximum penalty, in relation to individuals aged under 18 years. I would support such as measure on the basis that youths under the age of 18 are less likely to be able to fully understand the potential impact their actions can have on others on account of their developmental stage, notwithstanding the fact that a court would automatically take into account the age of a young person during sentencing.

Q22 Is there merit in establishing a new mid-range cyberullying offence applying to minors?

Where policy makers do not consider reference to cyberbullying appropriate in the context of section 474.17, the creation of a separate mid-range cyberbullying offence is an initiative which holds significant merit.

A specific offence would bring conceptual clarity to how cyberbullying is defined and understood. This would be highly significant given current definitional uncertainty. It is important to note, that cyberbullying differs from generally aggressive behaviours – specific criteria delineates cyberbullying from generally aggressive online behaviour (Langos, 2012). Another advantage of creating a specific offence is its communicative function — it's symbolic power. The expressive function of the criminal law can be employed to raise the profile of a particular issue in the community. It is one way 'social norms' can be shifted and is a means of drawing a blunt line as to what is unacceptable behaviour. A specific offence denounces conduct in an unequivocal manner. The media coverage associated with the enactment of a specific cyberbullying offence would initiate dialogue raising awareness of what cyberbullying is and the harmfulness associated with the conduct. It would raise awareness of the risks involved with Internet use generally, which would complement the current federal government 'cyber safety' initiatives and initiatives funded by private industry. Additionally, defining the nature and scope of particular conduct by creating a specific offence may assist police in identifying the forms of behaviours which warrant prosecution more easily.

I would support a proposition that such an offence be applicable generally, rather than being applicable to *minors only* as suggested in the consultation paper. Cyberbullying is not limited to a youth only context. However, I would support a provision in the legislation where by the maximum punishment for the offence is set at a lower maximum in relation to individuals under the age of 18. This has been the approach taken by various overseas jurisdictions in relation to the criminalization of cyberbullying (for example, the US state of Louisiana criminalizes cyberbullying, HB 1259 stipulates that the maximum penalty for a

person under the age of 18 is a fine, the maximum penalty for a person over the age of 18 is a term of imprisonment). It may be appropriate to set a maximum penalty, such as a fine and to order family conferencing where the offender and victim reside in the same state and where the victim consents. The potential benefits of family conferencing in relation to instances of cyberbullying are discussed by Langos (2013b). From an offender's perspective, the forum provides an offender with: an opportunity to divert away from the adversarial court process and avoid criminal prosecution; an opportunity to explain the circumstances of the offence; insight as to how cyberbullying has impacted on the victim; an opportunity for the offender to foster empathy for the victim; an opportunity for the offender to apologize to the victim; an opportunity to commit to specific undertakings as reparation for the offending conduct. From a victim's perspective, the forum provides a victim with: an opportunity to convey to the offender how cyberbullying has impacted them (harm caused); an opportunity to get some answers as to why they were victimized; an opportunity to hear the offender apologize; an environment which fosters voluntary forgiveness by the victim, which, in turn, may assist in healing psychological harm; a forum where certain undertakings are entered into on behalf of the offender. This may assist a victim in their recovery process in the fact that the offender will bear some responsibility for his or her actions, fostering a sense of justice and closure for the victim. The core premise of the conference is to repair the harm caused to the victim. Family conferencing is a workable diversionary response to instances of cyberbullying (Langos, 2013b).

In relation to adults, it may be appropriate to set a maximum penalty similar to the maximum 3 year term of imprisonment associated with section 474.17. This is primarily because of the fact that a specific cyberbullying offence should be narrowly tailored to

prevent over-criminalization. The seriousness (harmfulness) of the conduct likely to fall within such an offence justifies a penalty somewhere in this range.

Langos has drafted model cyberbullying legislation in the South Australian context (Langos, 2013b). The design of this legislation could, however, be applied to the federal context. The most important aspects of this model legislation relate to the provision of a *narrow* definition of 'harm' and the inclusion of the fault element of '*intention*'. A narrow statutory definition of harm will limit the scope of conduct likely to be captured by the offence. In a cyberbullying context, 'harm' is generally understood to include emotional harm which refers to a very broad range of emotions including: feelings of anxiety, distress, annoyance, apprehension, grief and anger. It may be relatively straight forward to prove a perpetrator intended merely to annoy or upset a victim. This low threshold of harm is likely to result in the prohibition of a range of intentional but otherwise fairly 'mundane' conduct. The requirement of the fault element of 'intention' limits the scope of an offence to the maleficent. The Model Criminal Code Officers Committee recommended in their *Report* of 1998 that the offence of 'stalking' required the criterion of intention to prevent over-breadth; prevent 'making a serious and stigmatising offence of very minor nuisance' (Model Criminal Code Officers Committee of the Standing Committee of Attorneys-General, 1998). This discussion has relevance in relation to cyberbullying, both offences being concerned with regulating anti-social behaviour which has varying degrees of harm (severity of harm) associated with the conduct. 'Intention' is an important criterion of both a 'bullying' and 'cyberbullying' (descriptive) definition. Without its inclusion, joking, jovial teasing, inadvertent/accidental behaviours are captured in an overly broad meaning of the terms. Although the subjective nature of 'intention' can make this fault element difficult to prove,

its absence would leave the scope of a cyberbullying offence open to ridicule on account of over-breadth, and may also give rise to the phenomenon of 'net-widening' ('mesh-thinning') developed by Stanley Cohen (Blomberg and Cohen, 2003).

A narrowly tailored specific cyberbullying offence would result in the exclusion of less serious instances of cyberbullying. The type of conduct likely to fall within the scope of the offence is sufficiently serious to warrant a penalty including a maximum term of imprisonment similar to that provided for in s 474.17.

Q23 Is there merit in establishing a civil enforcement regime (including an infringement notice scheme) to deal with cyberbullying?

I support a civil enforcement regime. The proposed Australian regime would complement criminal law initiatives; education campaigns; government and private industry cyber-safety initiatives. What constitutes as 'harmful' material ought to be defined *more broadly* than it ought in a criminal law context (but not so broadly as to encroach too severely upon the right to free expression/speech). This would enable a wider range of cyberbullying to be addressed. Infringement notices are appropriate under a civil penalty scheme, given the potential lower gravity of harm associated with the conduct youths, parents, school principals are likely to lodge complaints about.

This is an appropriate mechanism for dealing with less serious instances of cyberbullying which fall outside the scope of either a specific federal or state cyberbullying offence or general federal misuse of telecommunications offence. It is likely that one of the most productive aspects of such a civil enforcement regime will be the restorative focus (focus on

mediation between the cyberbully and the target of the cyberbullying) of the proposed system. Because of the public humiliation associated with cyberbullying, the ability of the Commissioner to order the removal of harmful online material is also a highly significant function.

Overall, of the potential initiatives, creating a separate offence for cyberbullying (Option2), along with the establishment of a civil enforcement regime (Option 3), hold significant merit. The initiatives complement each other and one ought not be implemented without the other in order to ensure a strategic, holistic response to cyberbullying is delivered. Raising awareness of cyberbullying, and misuse of online communications generally, ought to be addressed through education campaigns targeting youths and adults through the school context, the workplace and through mainstream media in the pursuit of keeping both children and adults safe in the online environment.

References:

1. Blomberg T and Cohen S (2003) *Punishment and Social Control*. New York: Walter de Gruyter.

2. Campbell M, Spears B, Slee, P, Butler, D and Kift S (2012) Victims' perceptions of traditional and cyberbullying, and the psychological correlates of their victimisation. *Emotional and Behavioural Difficulties* 17(3-4): 389-401.

3. Commissioner for Children and Young People and Child Guardian (2012) 'Child deaths - cyberbullying as a risk factor for youth suicide'. *Trends and Issues paper* 5 (March): 1-3.

4. Commonwealth Government (2011) 'Before it's too late: report on early intervention programs aimed at preventing youth suicide': Canberra.

5. Hinduja S and Patchin JW (2010) 'Bullying, cyberbullying and suicide'. *Archives of Suicide Research* 14(3): 206-221.

6. Juvonen J and Gross EF (2008) 'Extending the school grounds?—Bullying experiences in cyberspace'. *Journal of School Health* 78(9):496-505.

7. Langos C (2012) ‘Cyberbullying: the challenge to define’. *Cyberpsychology, behaviour and social networking* 15 (5): 285-289.

8. Langos C (2013a) ‘Which laws can apply to cyberbullying?’ *Bulletin* 35 (10): 38-40.

9. Langos C (2013b) *Cyberbullying, associated harm and the criminal law* (PhD Thesis). University of South Australia, Adelaide, South Australia. Retrieved from http://arrow.unisa.edu.au:8081/1959.8/151636.

10. Model Criminal Code Officers Committee of the Standing Committee of Attorneys-General (1998) *Chapter 5: Fatal Offences Against the Person Report*. Model Criminal Code officers Committee.

11. Perren S, Dooley J, Shaw T and Cross D, (2010) Bullying in schools and cyberspace: Associations with depressive symptoms in Swiss and Australian adolescents. *Child and Adolescent psychiatry and Mental Health* 4: 28.

12. Rigby K (2003) ‘Consequences of Bullying in Schools’. *Canadian Journal of Psychiatry* 48(9): 583-590.

13. Sourander A, Brunstein A, Ikonen M, Lindroos J, Luntamo T, Koskelainen M, et al. (2010) ‘Psychological risk factors associated with cyberbullying among adolescents: A population-based study’. *Archives of General Psychiatry* 67(7): 720-728.

14. Wang J, Nansel TR and Iannotti RJ (2011) ‘Cyber and traditional bullying: Differential association with depression’. *Journal of Adolescent Health* 48(4): 415-417.

15. Ybarra M, Mitchell K, Wolak J and Finkelhor D (2006). ‘Examining characteristics and associated distress related to internet harassment: Findings from the second youth internet safety survey’. *Pediatrics* 118(4): 1169 -1177.