the australian universities' anti-bullying research alliance (AUARA)

SUBMISSION TO

Australian Government
Department of Communications
Public Consultation on Key Election Commitments

Enhancing Online Safety for Children

Prepared by:

Dr Barbara Spears: School of Education, University of South Australia
Barbara.spears@unisa.edu.au

Professor Marilyn Campbell, Queensland University of Technology
ma.campbell@qut.edu.au

Professor Phillip Slee, Flinders University
Phillip.slee@flinders.edu.au

Professor Donna Cross, University of Western Australia
dcross@ichr.uwa.edu.au

Contents

The Submission According to the Terms of Reference:

As set out in the *Policy to Enhance Online Safety for Children*, the Australian Government is committed to establishing a range of measures to improve the online safety of children in Australia, some of which include:

- The establishment of a Children's e-Safety Commissioner
- Developing an effective complaints system, backed by legislation, to get harmful material down fast from large social media sites, and
- Examining existing Commonwealth legislation to determine whether to create a new, simplified cyber-bullying offence.

The Department of Communications (the Department) is seeking views on the issues raised in this discussion paper to assist in providing advice to the Government to enhance online safety for children.

Scope

This submission by AUARA, builds upon the national and international research foundations of our alliance in the fields of aggression, bullying and school violence, mental health and wellbeing and demonstrates the importance of quality research and providing an evidence-base in addressing the latest bullying iteration: cyberbullying and associated online safety concerns for young people in this country.

This Submission will specifically respond to the following and provide a general response in conclusion.

1.0 Establishment of a Children's e-Safety Commissioner

Q1: What existing programme and powers should the Commissioner take responsibility for?

Q2: Considering the intended leadership role and functions of the Commissioner, which option would best serve to establish the Commissioner?

3.0 Options for dealing with cyberbullying under Commonwealth legislation

3.1 Options for a Commonwealth cyber-bullying offence

Option 1: Leave the existing offence unchanged and implement education and awareness raising measures to better explain the application of the current offence.

Q 20: In light of the Government's proposed initiatives targeting cyberbullying set out in Chapters 1 & 2; do the current laws relating to cyberbullying require amendment?

Q 21: Is the penalty set out in section 474.17 of the Criminal Code appropriate for addressing cyberbullying offences?

Option 2: Create a separate cyberbullying offence covering conduct where the victim is a minor (under 18 years), with a lesser maximum penalty such as a fine.

Q22: Is there merit in establishing a new mid-range cyberbullying offence to minors?

3.2 Options for a Commonwealth civil penalty regime

Option 3: Create a separate civil enforcement regime to deal with cyberbullying modelled on the New Zealand "Approved Agency" approach.

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

Q24: What penalties or remedies would be most appropriate for Options 2 & 3?

Background to AUARA

The ***Australian Universities' Anti-bullying Research Alliance*** (AUARA) is a collaboration which aims to:

- inform policy and practice through quality evidence-based research; and to
- improve outcomes for young people in the areas of:
    - cyberbullying in particular, and
    - cyber safety in general.

AUARA comprises leading researchers from the following Universities (Alphabetical order)

- Flinders University (Professor Phillip Slee)
- Queensland University of Technology (Professor Marilyn Campbell) and
- University of South Australia (Dr Barbara Spears)
- University of Western Australia (Professor Donna Cross)

The Alliance has significant international links with organizations concerned with the issues of online bullying (cyberbullying) and cyber safety including, among others, the:

- European Co-operation of Science and Technology: Action ISO801: *Cyberbullying: coping with negative and enhancing positive uses of new technologies, in relationships in educational settings.* (http://sites.google.com/site/costis0801/)
- United States Children's National Medical Centre (http://www.childrensnational.org/advocacy/KeyIssues/Bullying.aspx);
- Canadian PREVNet: Promoting Relationships and Eliminating Violence, National web site: (http://prevnet.ca/Home/tabid/36/Default.aspx) and
- International Observatory on School Violence (http://www.ijvs.org/)
- National Centre for Missing and Exploited Children (http://www.missingkids.com/missingkids/servlet/PageServlet?LanguageCountry=en_US&PageId=169) and the
- Bullying Research Network (BRNET) http://brnet.unl.edu

Context Statement

Online-safety is a complex issue and requires consideration of cyber safety, risk management and harm minimization in relation to such concerns as: cyberbullying, cyber-stalking, online grooming; sexting, privacy and identity theft among other harms online. It is a term which implies the safe and responsible use of technologies (See Campbell, 2005; Campbell, Spears, Cross, & Slee, 2010). As a multimodal medium (text, image, video, sound), embracing messages, chats, photo albums, blogs, and other applications, it is a particularly attractive medium for children and young people and it is reshaping and reframing the presentation and management of young people's identity, lifestyle and social relations (Spears et al., 2013).

Australia now has a generation of young people who have never been without online access and as such it is fully integrated into their lives (High Wire Act, 2011). They live, laugh, learn, interact, play and work straddling both online and offline environments, seeing it as "the one life" (Spears et al., 2012). The internet has fundamentally changed the way young people spend their time and the way they communicate with peers. The Australian Communication & Media Authority (ACMA) reports (2011) that over 95 % of young Australians use the internet regularly. Almost daily internet use is common for children as young as eight or nine. This rapidly changes in the 'tween' years with many 10-12 year olds using the internet from 1-3 hours per day. By 13 years of age, social media use has become the norm; and by 15, the internet and its use has become an 'organic integrated part' of the everyday lives of Australian children. Research evidence however (e.g. Byrne et al., 2014) shows that the increase in internet time is associated with increased exposure to on-line risk. The diverse range of technology now available to young people has been associated with a number of benefits to adolescents, such as opportunities for improved social communication (Costabile & Spears, 2012; Spears et al., 2012). In accordance with the growing use of electronic communication technologies among young people, however, is the increasing likelihood for such technologies to be misused and cause harm (Campbell, 2005; Smith et al., 2008).

Researchers have identified three types of risks young people may be exposed to while using the internet (i) content risks, (ii) contact risks and (iii) conduct risks (Livingstone & Haddon, 2009). such as: disclosing personal information, cyberbullying, receiving sexual messages

and online/offline contact with strangers. However, risk should be distinguished from actual harm. The EU Kids Online research indicates that about 12 % of children across Europe have experienced actual harm after exposure to online risks. Research shows that some children and adolescents have more difficulties in coping with these online risks and preventing themselves from being harmed than others (Livingstone et al., 2010; Brighi, 2012). Moreover, what is considered an online risk by adults is not necessarily perceived as a risk by adolescents (Livingstone & Helsper, 2008). In Australia the 2011 Joint Select Committee (High Wire Act) on cybersafety reports that the five major risks for young people are (i) cyberstalking, grooming and sexual solicitation (ii) cyberbullying (iii) exposure to illegal and inappropriate material; (iv) promotion of inappropriate social & health behaviours and (v) identity theft, privacy and online security. Australian research indicates that that while children and young people have a high awareness of cybersafety risks, e.g., the majority of teen SNS users have set their profile to private *although* 20% of 12-13 year olds have not. The likelihood of children and young people posting personal information on social networks *increased with age*—(28% of 8 -9 year olds SNS users) to 77 % of 14-15-year-old users and 79 % of 16-17-year-old (ACMA, 2012).

Baumgartner et al. (2010, p.1226) in their review of the research noted that "engagement in risk behaviours peaks during adolescence". Adolescents are over-represented in nearly every category of risk behaviour, such as drug use, alcohol consumption, smoking, skipping school, and unsafe sexual activities'. In their review of developmental research, Slee, Campbell and Spears (2012) have noted that the evidence is that young people take more risks than children or adults do but understanding why this should be has been challenging. Steinberg (2007, p. 51) has argued that recent advances in neuroscience would suggest that the 'inclination to engage in risky behaviour does not appear to be due to irrationality, delusions of invulnerability, or ignorance'. The same author has argued that risk taking in the *real world is the product of cognitive reasoning and psychosocial factors.* However, unlike logical-reasoning abilities, which appear to be more or less fully developed by age 15, psychosocial capacities that improve decision making and moderate risk taking—such as *impulse control, emotion regulation, delay of gratification, and resistance to peer influence*—continue to mature *and it is these elements that provide the focus of this research application.*

The rise of the internet may provide adolescents with *many new outlets to engage in risky behaviours*. As Spears et al. (2013) have noted, there are hidden risks for adolescents that many are unaware of after they have left their digital footprints on SNSs e.g., profile information and personal photographs. However, it would be erroneous to suggest that young people comprise a homogenous group in this regard and research would suggest that certain groups may be particularly 'at risk' for engaging in risky internet behaviour. Online risky behaviour can occur through the disclosure of information to strangers who abuse the trust given by the victims, or through the posting of personal information on social networking sites without much thought given to privacy and security settings available (Ybarra & Mitchell, 2008). Research in the privacy arena has shown that preteens and adolescents who are likely to engage in high-risk behaviour online are prone to online predators and objectionable content (Byrnes et al., 2014).

Australian schools will be receiving broadband connections, which will deliver internet speeds around 100 times faster than most current speeds in schools. While this technology will help to maximise the benefits offered by online curriculum content, the group most likely to be affected by cyberbullying, reputation damage and risk - high school age students – are the very same group who will have increased access through government policy to technology in schools.

Bullying in cyberspace has wide-ranging and potentially severe consequences. Of concern are those related to mental health, e.g., depression, lowered self-esteem, (e.g., Campbell et al. 2013). Such psychosocial and emotional harm due to online harassment can sometimes last longer than bullying experienced offline and the limitless boundaries of online harassment pose a daunting challenge not just for the victims themselves, but also for educators and policymakers in formulating policies about online harassment (e.g., Cross et al., 2011). Behaviours which are at the forefront of their online activity, are those related to bullying and manipulation of their peer relationships. Bullying is a complex, ongoing societal issue that requires a multi-faceted, whole of community prevention approach. It is a relationship problem which requires relationship solutions, so is not the sole responsibility of any one individual or group: it also requires a system level and whole-of-government response (Cross et al., 2009; Campbell et al., 2010; Slee et al., 2011; Spears et al., 2008, 2009).

There is growing understanding that serious online problems may be indicative of a broader pattern of problem behaviours and/or underlying emotional issues for youth, and vice versa. For example, previous research (e.g,. Campbell et al., 2013) has determined that young people engaging in bullying others on-line and being victimised on-line experience social and emotional problems. Lewin et al. (2013) has noted that it is also not known 'if there are subsets of youth for whom new technology provides an environment or opportunity for problems to occur when they might not have otherwise'(p.269). It is reasonable to argue that young people who take risks in one area of their lives (e.g., SNS) will also take risks in other areas.

As adults and governments, we share a responsibility to provide an evidence-based, educative approach, which will maximize positive and minimize negative impacts of being active in an online environment. This requires, therefore, an understanding of young people and how they interact socially and emotionally, and recognition by adults that young people today behave and relate to each other in ways they have always done, except that this is now done through and surrounded by, various forms of technology (Slee, Campbell, & Spears, 2012). Working across systems such as health and education, offer opportunities for embedding the key cyber-safety, mental health and wellbeing prevention and intervention messages in the broader community, and support relationship solutions.

Keeping young people safe online, through cyber-safety education and supporting them to develop into ethical, digital citizens, where they can successfully navigate rapidly changing technological environments is however, a challenge (boyd, 2010; Costabile & Spears, 2012; Cross et al., 2009; Spears et al., 2008, 2009) . Young people, by their very nature are: exploratory; inquisitive; fun-seeking; playful and creative. At the same time, they can be devious and secretive in their behaviours; distrustful of adults and engage in risk-taking activities (Slee, Campbell, & Spears, 2012). There are developmental factors also which need to be at the forefront of any considerations in regard to cybersafety and cyberbullying and the cognitive, emotional, social and physical dimensions of young people as they progress from childhood through adolescence. Neuro-science also plays a part in this understanding, as there are significant changes to the brain occurring during adolescence, which impacts on their ability to make safe decisions, evaluate risks and regulate emotions (Slee, Campbell, & Spears, 2012).

Of the *possible protective factors* that might mitigate online risks, parents and their role in promoting children and young people's safe Internet behaviour has been *the focus of limited research* (Brighi et al., in press). *S*urveys of parents on their attitudes towards the Internet suggest that parents are anxious and insecure about their adolescents' use of the Internet (Liau, 2005; Downey & Brighi, in press). The research (Liau, 2005) suggests that parents tend to overestimate the amount of parental supervision and communication regarding Internet safety that occurs at home. A pilot study by Mubarak (2013) identified a wide communication gap existing between teenagers and their parents in relation to teen use of the Internet . *Hence, more research needs to be conducted to examine the nature and extent of parental Internet supervision, and whether higher levels of parental supervision is related to lower levels of adolescent engagement in risky Internet behaviours*. Another protective factor cited concerns the *level of digital literacy* and users' abilities to evaluate messages critically (or employ strategies to gain control over self presentation). However, limited research has found the opposite, primarily because skills enhance the range and depth of young people's online activities (and vice versa), and more diverse activities are unsurprisingly linked to more, not fewer, risk encounters *highlighting the need for further research* (Livingstone & Haddon,2008).

In contrast to promoting punitive based solutions to cyberbullying such as withdrawing access to technology, which may exacerbate the problem, it is suggested that raising the awareness among students, parents and educators, of the harms associated with the misuse of technology and providing strategies to minimise this harm, whilst providing opportunities for students to experience, learn from and benefit from new communications technology, may be key to reducing this insidious form of bullying amongst young people (Campbell et al., 2010; Cross et al., 2009, 2011; Slee et al., 2011; Spears et al., 2008,2009).

Hence, interventions which aim to increase online safety need to foster positive behaviour in adolescents using a harm minimization approach. This harm minimization approach recognises that participation in cyber space is a naturally occurring phenomenon in adolescents, and rather than eradicate its use altogether, focuses on reducing the potential hazards of use of new communications technology. Rather than merely passively informing schools and parents of safety guidelines, interventions need to actively encourage adolescents

to explore concepts of "netiquette" and the interplay between identity, trust and deceptions within the virtual world, enhancing their ability to assess the reliability of information and the trustworthiness of a confidant.

Schools need help to build bridges between social and emotional learning (SEL) which supports mental health and cyber-safety and cyberbullying initiatives/strategies which act to keep children and young people safe online. Improved social and emotional learning not only improves wellbeing, however, it also increases academic outcomes and reduces risk, which are clear imperatives for any government.

The National Safe Schools Framework (NSSF) (2003; 2011) is unique in the world as it advocates building positive *community* responses, *building on strengths* and *restoring relationships*, all of which are required for a functional citizenry. This framework determines that safe schools offer greater opportunities for improved learning outcomes. It establishes that everyone involved with schools: students, teachers, school leaders, administration and parents, has the right to safe and supportive teaching and learning environments. The NSSF is also not the domain of any individual research or political agenda, which is important in terms of continuity of messaging around the issues of cybersafety and cyberbullying.

However, schools are not the only place where interventions and education can and should occur. Young people are engaged in "*networked publics*" (boyd, 2010), places where young people congregate online, and where their social dramas play out. Reaching young people *wherever* they are will be of importance (Spears & Zeederberg, 2013) , and whilst schools are significant places of learning and sharing, they need to be seen as part of a community response to cybersafety and cyberbullying, and not the sole provider of all intervention strategies.

The aim is to continue to grow community, citizenship and respect, and Australia is seen as a "lighthouse" in national prevention approaches, working in a proactive and restorative manner, rather than employing only a legalistic process. Whilst a legalistic understanding is necessary, it is the nexus between the law and what is in the best interests of our young people that requires careful consideration. Laws which relate to offline behaviours do not readily translate to online interactions. Boundaries are blurred between home and school, across countries and therefore jurisdictions, so the serious question regarding the

criminalising of our children needs to be considered. Anti-bullying policies at the school level require examination in terms of cyberbullying, to ensure that the community knows and understands what is acceptable and what crosses the line (Butler et al., 2011).

Limited research evidence inhibits the effective decision making of legislators, policy makers, schools and families about cyber bullying and cybersafety. It is imperative that a "one-size fits all" model of intervention is not adopted. Change is ubiquitous in this environment. Online bullying, reputation damage and risk will be constantly evolving and it requires ongoing research to find ways of minimising harm and reducing risk with each generation of young people as they progress developmentally through their normal adolescent milestones.

It must also be noted, that researchers, policymakers and practitioners, reflect three related yet distinct cultures when it comes to understanding and improving matters of health and wellbeing for children and young people (Shonkoff, 2000). Researchers and scientists are engaged in answering questions and policy makers utilise such knowledge to support political, economic and social agendas. Practitioners, on the other hand, are focused on the delivery of services, borne out of the research and enshrined in policy, but employed within confined budgetary and economic boundaries. It is the job of each, to unite to find the best ways possible of achieving positive outcomes for Australia's young people, particularly in regard to the ever-changing online environment.

Consideration of the cumulative, positive impact and effects of the initiatives which have grown across time and governments, highlight the need for an ongoing approach which builds upon previous research and policy, so that community gains are not lost. Most importantly, young people should be at the centre of everything we do (Spears et al., 2011).

Managing the tension between the need to provide continued, up to the minute technological development, through capital grants to school systems, and community infrastructure in order to ensure world class information and communications technologies, against the need to also provide appropriate levels of education, support and constraints in schools and homes, is a formidable task, especially as the very need for the technology may present young people with increased opportunities for technology-based harm.

The previous Labor government's approach *built upon the strong foundation* provided by previous Liberal government which initiated *Net Alert* (1999) and the *National Safe Schools*

Framework (2003) and provided funding for *the Australian Covert Bullying Prevalence Studies* (Cross et al., 2009; Spears et al,.2008; 2009). Labor then provided: the *National Cyber-Safety Plan* (2008, Department of Broadband, Communications and the Digital Economy), which included the merging of *Net Alert* into the Australian Media and Communication Authority's *Cybersmart* initiative; and the re-writing of the *National Safe Schools Framework (2011*) to include issues of cyberbullying and cybersafety. Other initiatives such as the formation of the *Consultative Working Group* (2008) which brings industry partners together with policymakers and government representatives, and the *Youth Advisory Group* (2009) which provides much needed youth voice and perspectives to the issues of online bullying and reputation damage and risk, have emerged as the social media environment grew, and new challenges were faced by young people's engagement online. The *High Wire Act: Cyber-Safety Report of the Joint Select Committee on Cyber Safety (2011)* highlighted the ongoing and changing issues for young people in a technological environment which has moved from the static, text-based search engines of the early internet in the 1990s, to the mobile, highly interactive, publishing capabilities of contemporary social media.

The challenge for any government is to recognise the value in what has been done to date, to then find ways of building upon it in response to changing community needs, mindful that there will always be a new group of 13- year-olds who begin their adolescent journey, faced with different technological capabilities to the previous generation.

Definition of Cyberbullying

There is no universal agreement on definitional issues amongst those researching the topic of bullying. Cross-culturally there are differences in how bullying is understood and whether in fact there is a word in some cultures for 'bullying' . Developmentally children and young people also describe bullying in different ways with younger children having less differentiated ways of describing bullying than adolescents. There is also a suggestion that gender has an impact on how bullying is understood with females focussing more on the relational component and males on the physical element. In mainstream western culture there is now some general degree of consensus by adults that bullying refers to behaviours that hurt or harm another person, with intent to do so; the hurt or harm maybe physical or psychological and is repeated; and there is a power imbalance (social, psychological or physical) such that it is difficult for the victim to defend him- or herself. Most recently, the

latest iteration of bullying: cyberbullying, involves the deliberate (mis)use of technology to target another person. Bullying is thus a relationship characterized by continued aggression and with a power asymmetry. However, it has been argued that behaviour which is not necessarily intended by the perpetrator to cause hurt or harm, may be considered as bullying if it is taken as such by the victim. Definitional issues are further complicated in as much as researchers do not all advocate that that an incident has to be repeated in order to be considered as bullying, especially if one incident causes long lasting fear of repetition. In relation to cyberbullying one incident that goes 'viral' could be considered 'repetition.

1.0 Establishment of a Children's e-Safety Commissioner

The Government's election policy committed to the appointment of a senior Commonwealth official as a Children's e-safety Commissioner (The Commissioner), supported by existing resources reallocated from existing locations within public service. The Commissioner will be a single point of contact for online safety issues for Industry, Australian children and those in charge of their welfare. The Commissioner will also take the lead across government in implementing policies to improve the safety of children online (Discussion Paper, p5).

1.1 Functions of the Commissioner

The Commissioner will have responsibility for:

- *implementing the proposed scheme for the rapid removal of material that is harmful to a child from large social media sites*;

Comment:

The rapid removal of material from large social media sites, that is harmful to a child, is, in essence, a sound, common-sense approach, however, it currently relies on the goodwill of the industry, and clear, mutually agreed understandings of what comprises harmful material to children and young people. From a developmental perspective, a younger child seeing video footage of an animal being injured or mistreated, or a vehicle accident, or accidentally stumbling across war-zone reporting may be emotionally or psychologically harmed by it. It would be impossible and unrealistic to seek rapid removal of material such as this, yet it is a cyber safety consideration: *how to ensure that online safety is enhanced for children of all ages, and they are protected in their dealings with the online setting.* To this end it would be important that the time of the Commissioner is not wasted, and one way that this level of online safety might be supported, is through reviews of all Child Protection Curricular across the States. Recently, the South Australian Keeping Safe: Child Protection Curriculum was reviewed, with a focus on including ways of keeping children and young people safe *online*. A clear recommendation made, was to encourage a stronger national focus on cyber safety, with more strategies and options available for children and young people to report issues.

AUARA would expect the Commissioner to have oversight and advocacy as his/her leading brief, and not be the actual hands-on complaints person. The Commissioner is needed to engage in higher level advocacy for enhancing children's online safety, and would need to be supported by those who would activate the take –down orders.

- *working with industry to ensure that better options for smartphones and other devices and internet access services are available for parents to protect children from harmful content*;

Comment:

Given that parents are either directly purchasing or handing-down phones to their children as they upgrade, it is important that they take some responsibility for the technology that they unleash on their children/young people. Some simple to understand instruction sheets for parents on current capabilities, or setting up controls and filters which accompany the purchase of smartphones and other devices could be beneficial. Many parents, for example, were quite unaware that the internet could be directly accessed through some gaming consoles. Parental education programs about the technology they purchase and pass on, are equally as important as education/information programs for children and young people about their online safety.

AUARA would expect the Commissioner to work at the highest levels of Industry, in order to secure the best possible outcomes for young Australians.

- *establishing an advice platform with guidelines for parents about the appropriateness of media content;*

Comment:

The Cybersmart portal/programme from ACMA is an excellent example of a "one-stop shop" for parents, teachers and young people. It needs to be continued to be supported to provide the very high quality of evidence-informed materials and outreach it is currently providing to parents, young people and schools across the country. There would be no need to provide an additional advice platform for parents, if Cybersmart were to continue to operate as the main national online safety and security education programme/provider for such resources. It makes no sense to reinvent the wheel when it is unnecessary to do so. ACMA provide a raft of resources, research, initiatives and a highly skilled and nuanced team who have created a world-class online presence.

AUARA sees no reason to establish an additional advice platform, as we would expect to see ACMA retained as an independent body to continue to do the cybersafety work they have been doing: i.e. liaising with teachers to optimise materials, and centring young people in everything that they do.

- *establishing a research fund to consider the effects of internet use on children, how support services can be provided online and how to mitigate children's online risks*

Comment:

This will be an import and ongoing commitment by government. As the rapid innovation, convergence and uptake of new technologies will continue to roll out, there will never be a time when we know everything there is to know about how this and other emergent technological phenomena intersect with offline social interactions, education, physiology and relationships. More importantly, there will be a need to explore the impact on human brain function, and emotion development and regulation. Studies already demonstrate that individuals who are socially rejected, suffer pain responses in the brain, similar to those who have been physically harmed: http://www.independent.co.uk/news/science/brain-treats-rejection-like-physical-pain-say-scientists-8884507.html

By contrast, there is also evidence that video-gaming can be good for you: http://www.yawcrc.org.au/news/article/240

Understanding long term impact of any emerging technologies will require funding of large scale longitudinal studies, which explicitly focus on the positive and negative effects of technology over time.

An open, ground-up process for funding, similar to the way in which the *Cooperation in Science and Technology (COST)* (http://www.cost.eu/) scheme in Europe operates, would lead to innovation which would set Australia apart from the rest of the world. Having researchers come together around real problems to solve, rather than tendering for discrete projects put out by Government, means that the drivers of research are innovation and necessity, and are founded upon collaboration: imperatives for research into online behaviours such as cyberbullying and safety

- *establishing a voluntary process for the certification of online safety programmes offered within schools;*

Comment:

There should be no need to establish a voluntary process for the certification of online safety programmes offered within schools, if schools activate and undertake their National Safe Schools Audit tool, and the Commonwealth government supports schools in meeting their mutual obligations of accountability and transparency. Schools currently have the opportunity to employ the Audit Tool from the National Safe Schools Framework/Safe Schools Hub, as a way of assessing their progress and establishing their areas of risk and strengths in both the offline and online settings. The NSSF is an internationally significant approach, and places Australia at the forefront of work in this area. However, unless there is some mandated reason to complete the audit tool, and to do something with the data, it will not be widely used as it is intended: as a risk awareness and risk control process. The NSSF was updated to include cyberbullying in 2011, but it will need a continuous cycle of review, in order to be abreast of ongoing technological developments in relation to Safe Schools. If completion of the Audit Tool required submission of the data to an independent data analyst, certification to the school could then ensue, and the nation would then also have a significant picture of what is happening in our schools.

AUARA believes that this is preferable to having a separate user-pays system of voluntary certification: which is inequitable and an unnecessary cost for schools. Using the NFFS Audit tool, regularly updated to accommodate changes in contemporary school settings and children's behaviours relative to online environments (e.g. the shift from Web 1.0 to Web 2.0 to mobilisation of technologies) would be a cost effective, user-driven way of establishing a certification process which could then be easily linked with online safety programmes.

- establishing a funding programme for schools to deliver online safety education.

Comment:

Some caution is expressed here, lest all schools finance the "guest speaker/train the trainer" model, which is known to be relatively ineffective. Alternatively, a heavy reliance on "buying-in" expertise, might result in only one or two providers monopolysing the space, with the potential for some very ordinary and ineffective messaging being delivered. A plethora of marketing for product-placement occurring at the school gate is also to be avoided.

Whilst a specific online safety funding programme could be extremely beneficial if it were to be student-centred and co-designed with researchers, the experience from the United States is to be avoided: in certain states, cybersafety programs are mandated for schools and so they become the lobbying focus of many companies who have all manner of school-based 'resources' to sell them.

AUARA would expect to see school-based funding for student/youth led projects which developed their awareness and skill sets in addition to schools developing their own practitioner-researcher skills, in collecting evidence about their own practice and place.

In addition to the functions outlined above, there are a range of existing Australian Government online safety resources and programmes which could be transferred to the Commissioner's control.

Comment:

Noting the cyber safety programmes and resources listed in Appendix A of the Discussion paper (pp26-27), this submission recommends that:

- The ACMA remain the stand-alone authority and provider of key online education programmes, developmentally relevant initiatives, and high quality research related to internet use by children and young people.
- Their administration of the Online Content Scheme, which provides a complaints-based scheme for offensive and illegal content with power to issue take-down notices should also remain independent of the Commissioner.

It is absolutely counterproductive to dismantle such a successful unit, for the sake of streamlining, when it exactly meets the requirements of the Commonwealth government's policy direction: of enhancing online safety for children.

Bringing the other programmes and resources together, as listed in Appendix 1under the umbrella of the Department of Communication and/or the e-Safety Commissioner seems a valid response, as there is duplication of the resources and programming, albeit with different audiences in mind. This is not to say however, that the development of ongoing resources and programmes outside of the Commissioner's control would not occur, but they would be in the realm of Non-government providers, Not-for-Profit Organisations, or University Research Institutes and collaborations (e.g. Cooperative Research Centres; Australian research Council Grants) to name a few.

AUARA recommends that the ACMA remains outside of the Commissioner's control, and that its resources be suitably supported so that it can continue its highly acclaimed work.

Q1: What existing programme and powers should the Commissioner take responsibility for?

Response:

Having a single organisation which takes the lead in relation to online safety for children, will allow greater efficiency and address overlap and duplication.

However, there is a case to be made for retaining the independence of the ACMA and their suite of programmes, initiatives and research, including their online content scheme, with its powers to issue take down notices.

This is the body which has considerable expertise in regulating online content in this country, and it is greater than the sum of the other parts/programmes, in that it is not simply creating resources for the public consumption, but is an integrated entity with reach across and through our screens, working closely with all other relevant bodies, such as local and international police in instances of child grooming, to outreach educative programmes for pre-service teachers.

AUARA expects that the Commissioner should have an advocacy role and powers similar to other Children's Commissioners, rather than being a hands-on complaints adjudicator.

1.2 Establishment of the Commissioner

Options:

1: establishment of an independent statutory authority:

- the creation of a new independent statutory body, separately staffed to support the Commissioner and its functions: greatest level of independence but highest cost

2: establishment of an independent statutory office, with administrative support from an existing government agency

- the Commissioner would be established as an independent office, and support would be provided by an existing government agency. Administrative support could be provided by the ACMA or the Department of Communications, but consideration needs to be given to the perceived or actual independence from government.

3: designation of a Member of the ACMA as the Commissioner

- appoint an existing member of the ACMA Board to be the Commissioner, legislative amendments to the ACMA Act are needed; to be permanently within the ACMA , with distinct functions and powers to achieve the Commissioner's intended purpose. A temporary appointment would fast track transition to a new arrangement. A variation would be the appointment of an Associate Member of ACMA as the Commissioner, this would not require legislative amendment to the Act

4: designation of a non-government organisation with expertise in online child safety

- establish a legislated framework for appointing an expert non-government organisation (NGO) to undertake the role of the Commissioner; selected on a competitive basis; operating on a contractual basis: this is similar to the New Zealand approach under the new *Harmful Digital Communications Bill*.

Q2: Considering the intended leadership role and functions of the Commissioner, which option would best serve to establish the Commissioner?

Response:

AUARA supports Option 3: *the designation of a member of the ACMA as the Commissioner*. This enables the existing structure to carry on its excellent work as the Commissioner is appointed, and for the Commissioner to be independent of the Government. An Associate member is not supported. If this is a key initiative of the Government, then it needs to be legislated as permanently within the ACMA.

Option 1 is not supported, as this is far too costly and effectively disrupts the effective work being done currently by ACMA

Option 2 is not supported as it would stretch the resources of ACMA and shift its focus from its core business. The lack of independence is a significant issue.

Option 4 is not supported. Operating on a contractual basis suggests that this position can then be at the behest of any government, and is not a permanent feature of our cyber-safe landscape.

2.0 Rapid removal of material that is harmful to a child from social media sites

Context:

The Government proposes to introduce a scheme to enable the rapid removal from large social media sites of material targeted at and likely to cause harm to a specific child (the proposed scheme). The proposed scheme will provide an independent and impartial third party to consider such disagreements between social media sites and individuals on content complaints, where the content relates to a specific child in Australia. By establishing the proposed scheme in legislation, it will help to build the confidence and trust of Australian families in how social media sites deal with their concerns.

An issue that must be considered in this context is the ability to enforce compliance with a new regulatory scheme on foreign businesses. While the proposed scheme does not specifically target foreign businesses, the majority of large social media sites that would be affected by any rapid removal scheme operate from foreign jurisdictions. This issue is discussed at greater length under 'Penalties and Enforcement', below.

In addition to social media sites being required to remove material that is harmful to a specific child, it is proposed that individuals who have posted material to social media sites may also be required to remove material that is harmful to a specific child.

Comment:

AUARA acknowledges that the current role of ACMA includes the Online Content Scheme, which is set out in the *Broadcasting Services Act, 1992* and provides a complaints-based scheme for offensive and illegal online content with power to issue take-down notices. This is a system which has operated reasonably effectively to date, largely through the good relationships between the various departments. However, as social media continues to grow rapidly, the plethora of social media sites and the need to be across them sufficiently well, is increasingly difficult.

Fast take-down service is becoming increasingly important where children are concerned and AUARA supports the notion of a rapid removal approach, however also acknowledges the

difficulties of working with off shore providers/owners, who do not have the levels of community engagement which some of the larger social media companies do.

Giving the Commissioner powers to operate under safe harbour provisions, akin to those proposed in New Zealand seems a logical addition to the Online Content Scheme under the Broadcasting Service Act, 1992.

3.0 Options for dealing with cyber-bullying under Commonwealth legislation

3.1 Options for a Commonwealth Cyberbullying offence

Option 1: *Leave the existing offence unchanged and implement education and awareness raising measures to better explain the application of the current offence.*

Comment:

The biggest questions for AUARA are not whether we leave existing offences unchanged, or if we create a new simplified offence but the more relevant questions of:

(1) Do we want to criminalise our children?

(2) Is the use of the criminal law in the best interests of children and young people?

Legal remedies in themselves are not a solution to bullying, but are a necessary part of the solution.

Defining the legal rights and responsibilities of schools in responding to bullying and cyberbullying situations, and cyber-defamation is also important, as it is not only the child/young person perpetrating or being cyber/bullied which needs consideration. Whilst a case of minor/adult cyberbullying, defining the rights and responsibilities of all is of import.

Challenging Thought: Minor to adult cyberbullying

http://www.smh.com.au/technology/technology-news/the-tweet-that-cost-105000-20140304-341kl.html

A NSW school teacher has made legal history after a former student was ordered to pay $105,000 for defaming her on Twitter and Facebook.

In the first Twitter defamation battle in Australia to proceed to a full trial, District Court judge Michael Elkaim ruled that former Orange High School student Andrew Farley should pay compensatory and aggravated damages for making false allegations about music teacher Christine Mickle.

Judge Elkaim said the comments had had a "devastating effect" on the popular teacher, who immediately took sick leave and only returned to work on a limited basis late last year

The considerations below are therefore an important part of our response to Q 20 in relation to Option 1. They are taken from:

Kift, S., Campbell, M., Spears, B. Slee, P. *The existing criminal law in Australia for cyberbullying: Is there a need for change?* Presentation at the National Bullying, Young People and the Law Symposium, July, 2013Melbourne.

What are some of the current criminal laws in Australia that could deal with cyberbullying?

Commonwealth Law – e.g. *Criminal Code Act 1995* – misuse of telecommunication offences

State and Territory laws dealing with harassing, threatening, intimidating behaviour – e.g.

- Stalking offences
- Threat offences(more recently)
- Criminal privacy breach (re unauthorised visual recording and publication)

Other – e.g. child pornography; assault; blackmail; torture

Challenging Thought*: R v DW and KPD* (2002), Rounthwaite CJ asked–

"*When do school yard taunts cross over the line to become a criminal offence of threatening death or bodily harm?*"

When does a teenager's annoying behaviour towards a fellow student amount to an offence of criminal [stalking]?

E.g. ***Stalking (and like) Offences***

- Stalking broadly – "pursuit by one person of what appears to be a campaign of harassment or molestation of another" (Wells, 1997)
- Directed at conduct that may otherwise be beyond reach of criminal law
- Effective re cyberbullying because:
    1. Breadth of (stalking) behaviour captured is very wide
    2. Generally, intent required of stalking offender is that s/he intends to induce in target apprehension or fear of violence

    AND most Australian states include intention to cause either physical *or* mental harm

    1. Immediacy element required for threatened (criminal) assault is irrelevant
    - Many offences specifically now include cyber examples
    - Extra-territoriality issue (cf Vic) not such a problem re schools

Examples to consider:

SA Cyberstalking **SOUTH AUSTRALIA: *Criminal Law Consolidation Act 1935***

s 19AA

(1) A person **stalks** another if—

(a) on at least two separate occasions, the person—

(iva) publishes or transmits **offensive material by means of the internet or some other form of electronic communication** in such a way that the offensive material will be found by, or brought to the attention of, the other person; or

(ivb) communicates with the other person, or to others about the other person, **by way of mail, telephone (including associated technology), facsimile transmission or the internet or some other form of electronic communication** in a manner that could reasonably be expected to arouse apprehension or fear in the other person;

(b) the person—

(i) intends to cause **serious** physical or **mental harm** to the other person or a third person; or

(ii) intends to cause **serious apprehension or fear.**

Tasmania Cyberstalking **TASMANIA: *Criminal Code Act 1924* 192. Stalking**

(1) A person who, with **intent to cause** another person physical or **mental** harm or to be apprehensive or fearful, pursues a course of conduct made up of one or more of the following actions:

(g) publishing or transmitting **offensive material by electronic** or any other means in such a way that the offensive material is likely to be found by, or brought to the attention of, the other person or a third person;

(h) **using the internet or any other form of electronic communication** in a way that could reasonably be expected to cause the other person to be apprehensive or fearful;

(i) contacting the other person or a third person **by postal, telephonic, electronic or any other means of communication**;

QUEENSLAND: *Criminal Code Act 1899*

s 359B(c)(ii) – "*contacting a person in any way, including, for example, by telephone, mail, fax, e-mail* ***or through the use of any technology***"

Does the criminal law recognise psychological harm?

Uncertainty regarding this was a key driver for enacting legislation

E.g. Under *Queensland Criminal Code* stalking needs to cause apprehension or fear, reasonably arising in all the circumstances, or 'detriment'.

s 359A – "**Detriment**" includes:

(a) Apprehension or fear of violence to, or against property of, the stalked person or another person;

(b) **Serious mental, psychological or emotional** harm;

(c) Prevention or hindrance from doing an act a person is lawfully entitled to do;

(d) Compulsion to do an act a person is lawfully entitled to abstain from doing.

***Challenging Thought**: First Cyberbullying Case*

'His name was Allem Halkic and he was 17. When he made the decision to end his life at dawn last February, threatening text messages from a former mate weighed heavily on his mind.

"I'll put you in hospital," said one. "Don't be surprised if you get hit some time soon," read another.

Yesterday, Allem's former friend, Shane Phillip Gerada, avoided jail in Australia's first prosecution over cyber bullying. But a magistrate sent a warning to potential cyber bullies after the court heard that between 10 and 30 per cent of young Australians had fallen victim to the practice, described by a prosecutor as a "plague on the community"'

http://www.theage.com.au/victoria/man-avoids-jail-in-first-cyber-bullying-case-20100408-rv3v.html

More recently: Offences re criminal privacy breach

***Qld Criminal Code* – (ss227A-227B)**

- Offences re observing or visual recording in breach of privacy where reasonable adult would be expecting privacy or engaged in a private act (2 yrs)
  - Also **distributing** prohibited visual recordings (2 yrs)
  - "Private act" – "showering, bathing, using toilet, activity when in state of undress or intimate sexual activity not ordinarily done in public"
  - "Visually record" – "record, or transmit, by any means, moving or still images of the person or part of the person"

SA *Summary Offences Act 1953*

Part 5A—Filming offences:

s 26B—Humiliating or degrading filming

s 26C—Distribution of invasive image

s 26D—Indecent filming

Vic *Summary Offences Act 1966;* Div 4A – Observation or visual capturing of genital or anal region

s 41A Observation

s 41B Visually capturing

s 41C Distribution of image

Assaults, intimidation and harassment at school (Crimes Act 1900 (NSW) s 60E)

- Offence where a person 'assaults, stalks, harasses or intimidates' any school staff or student '**while attending the school**'.
- Would include cyberbullying
- 'Attending the school' defined in s 60D(2):
  - on school premises for the purposes of school work or duty (even if not engaged in school work or duty at the time),
  - on school premises for before or after school care, or
  - entering or leaving school premises in connection with school work or duty or before or after school care.

Two other interesting developments

1 Vic Law Reform Commission *Inquiry into Sexting* (May 2013)

http://www.parliament.vic.gov.au/lawreform/article/944

- Specifically recommends **de**-criminalising sexting behaviour between young people
  - By amending the Vic child pornography offences to provide a defence where images of (i) accused only *or* (ii) accused not more than 2 years older than minor, engaged in lawful sexual activity
  - Advocate that all State, Territory & Com offences similarly be amended
- Suggest new Non-consensual sexting offence for non-consensual distribution
- Recommend a Digital Communications Tribunal (informed by NZ Law Reform Commission proposal for Communications Tribunal)

2 Significant issue of Workplace Bullying

Recent detailed attention to Workplace Bullying

- Anti-bullying measures in *Fair Work Amendment Bill 2013* (Com) do ***not create an offence of bullying***, instead identify actions & behaviours that might constitute bullying and enable FWC to make orders to stop bullying
- **Medium/technology neutral**:

e.g. *s 789FD When is a worker bullied at work?*
– if an individual or group of individuals "*repeatedly behaves unreasonably towards the worker, or a group of workers of which the work is a member; and…that behaviour creates a risk to health and safety*"

- "**Health**" defined as both physical & psychological health

Draft model Work Health and Safety Code of Practice for Preventing and Responding to Workplace Bullying

- All **behaviours** described (at p 6) are **technology neutral** though specific examples include cyberbullying
- "***Workplace violence*** *(ie, physical assault or the threat of physical assault) should be reported to the police because these are criminal matters.*" (at p 7)

Workplace Bullying – Cyberstalking *Crimes Act 1958 (Vic)* s 21A

- Amended June 2011 in response to death of 19 year old Brodie Panlock who ended her life after enduring a persistent campaign of bullying by three of her co-workers.
- **Cyberstalking** specifically included (s 21A(2)(b), (ba), (bb), (bc))
- Stalking also includes (in 21A(2) (da)-(dd))
  - Making threats to the victim
  - Using abusive or offensive words to, or in front of, the victim

- Performing abusive or offensive acts in the presence of the victim
- Directing abusive or offensive acts towards the victim.

- Stalking also includes acting in a way that could reasonably be expected to cause physical **or mental** harm to the victim, including causing the victim to self-harm (including suicide).
- Mental harm is defined as including **psychological harm or causing a victim to engage in suicidal thoughts**.

Broader international scene: a snapshot of anti-bullying legislation & the law

USA: Anti-bullying legislation should include an appropriate range of penalties, such as school suspensions, criminal sanctions, and/or the ability to request a protective order (Srabstein,2008).

Europe: In a review of anti-bullying legislation in European countries it was typically reported that in relation to cyberbullying that while many countries had no specific law in place, existing legislation already covered aspects such as stalking (Mora-Merchan & Jager (2010).

Philippines: In 2013 approved a bill that would prohibit bullying in elementary and secondary schools.

Japan: In June 2013 the Japanese Diet enacted a law aimed at preventing bullying & the law stipulates that governments must closely monitor the Internet for online bullying and cooperate with police if such harassment is considered criminal.

Youth Voice:

Insights from Young People about their understanding of Cyberbullying and the Law

Qualitative Case Study: Using Interpretative Methodology

Youth Voice and Insights about Cyberbullying and the Law: Information Rich Case: *Single Secondary School, N= 1200*

Convenience, Purposeful, Random Sample: N=204

Maximum Variation Sampling: Year/Sex/Class

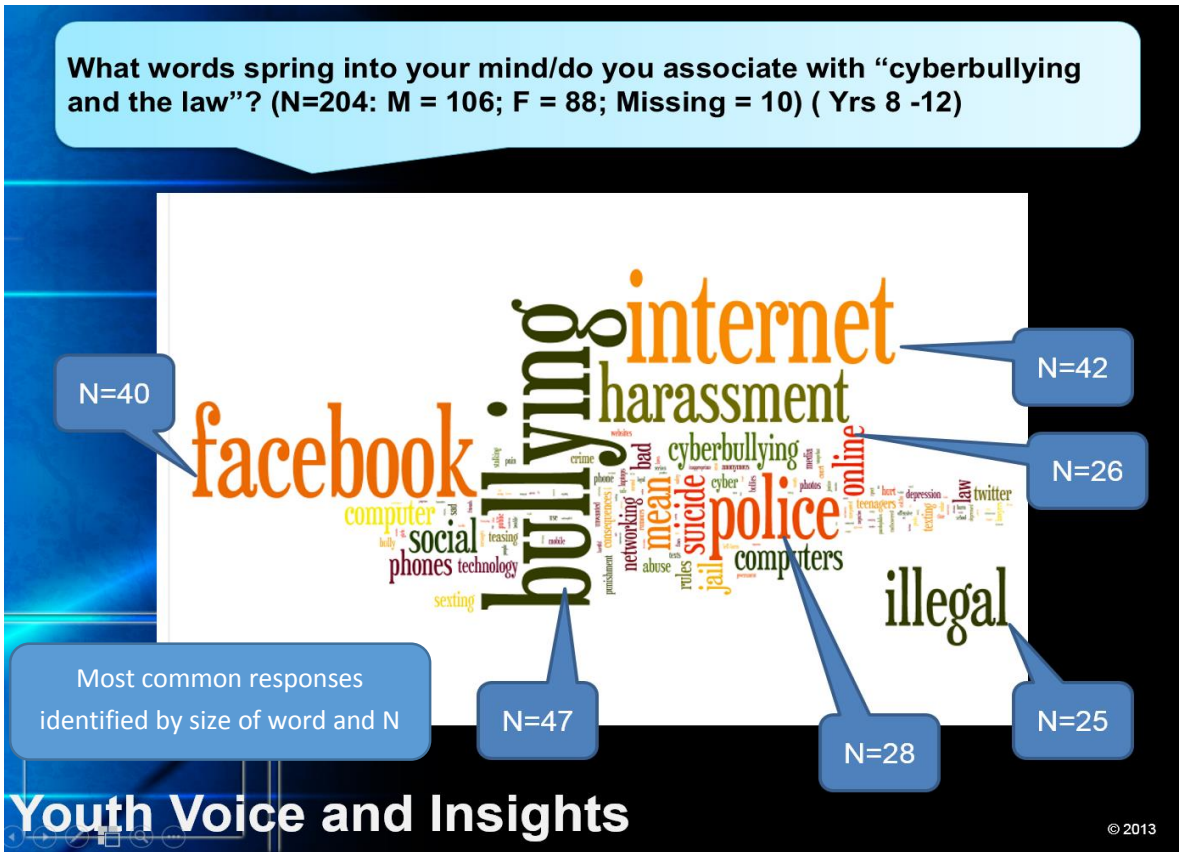
Leads to

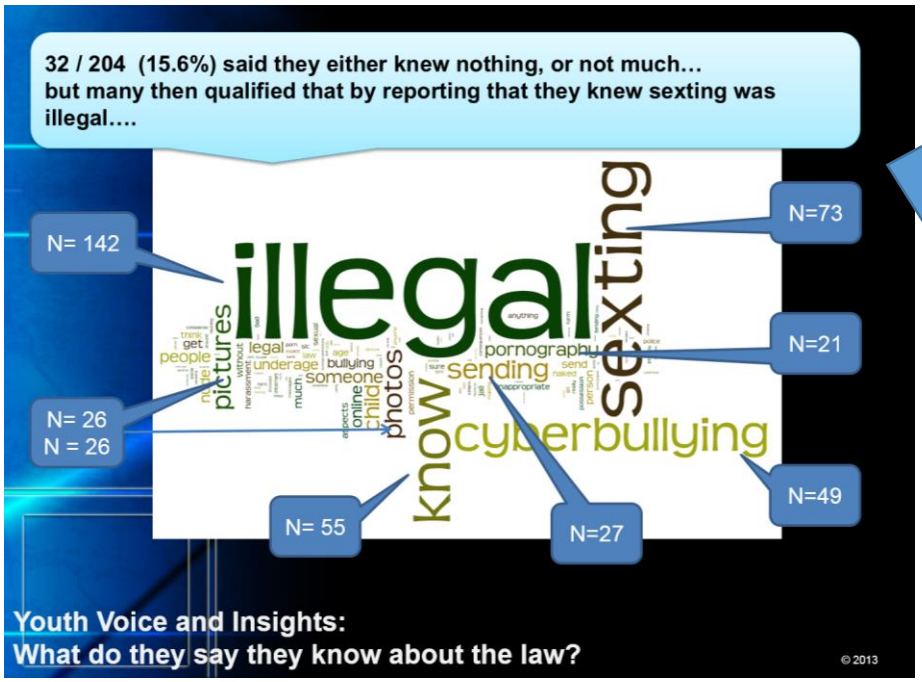
Key, Core Patterns emerging

Credibility of Findings

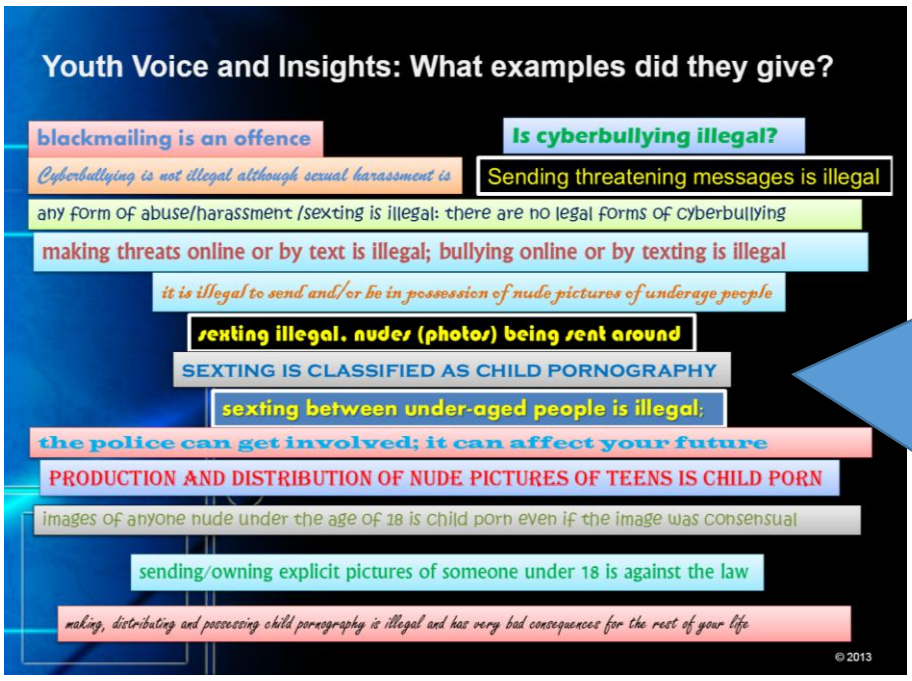
Saturation reached:

(no new information is forthcoming after several responses).



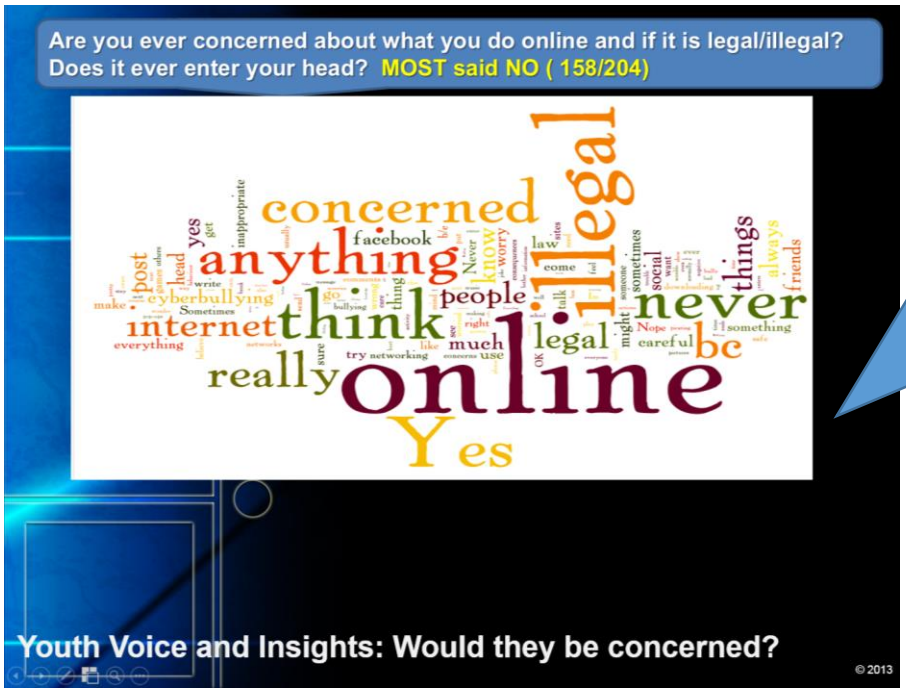


15% reported not knowing anything, or not much about CB and the law, but then qualified it by adding on that they knew that sexting was illegal



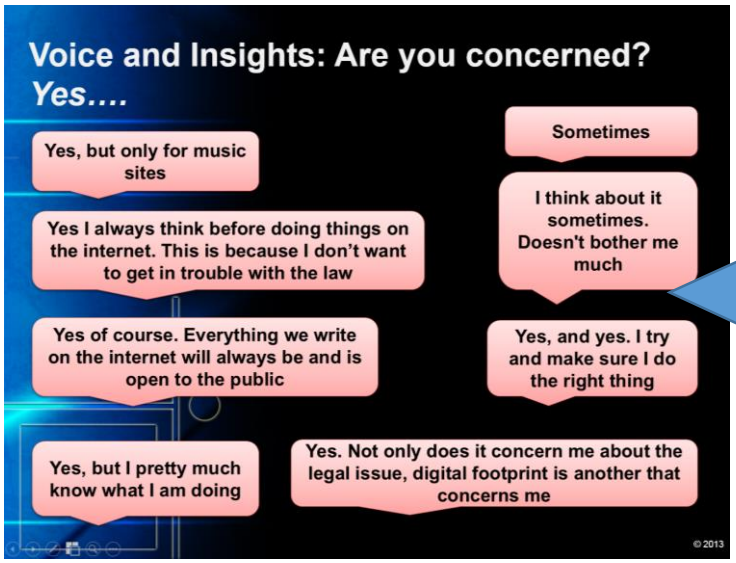
Their examples reflected the language they have heard in relation to sexting

e.g. *the production and distribution of child pornography*



Most (77%) were NEVER concerned about what they do online and if it could be illegal

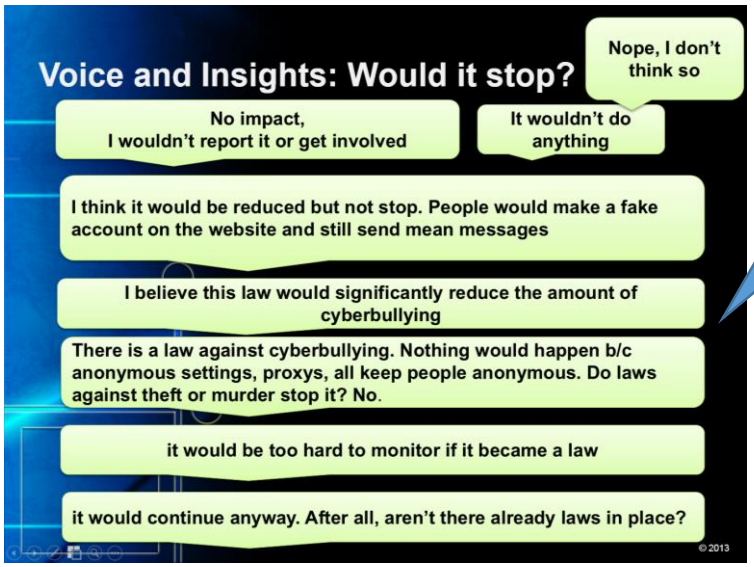
Reasons why they might not be concerned



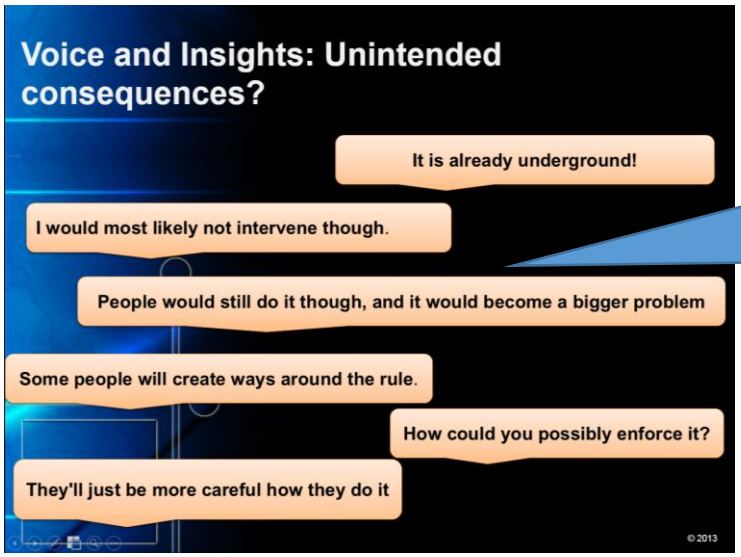
Reasons why they might be concerned:

Most related that concern to illegal downloads and not their

Most indicated that if Cyberbullying were to be a law, then they would report it.



But that having a law would not stop it happening



And that it might then go underground and they would find ways of circumventing it

Youth Voice Concluding Comments:

Young people know that there is a law to do with sexting, but not specifically cyberbullying, and they never think about their general behaviours as being potentially illegal when they go online.

If they do give it any thought, then it is in relation to illegal downloads, and not the interpersonal issues associated with bullying and cyberbullying. Some were of the opinion that there was a law for cyberbullying, but could not elaborate on it at all. The sexting information is cutting through in knowledge terms, but they have not distinguished sexting from cyberbullying.

What are the implications of existing laws for Schools?

NZ Law Reform Commission

Challenging Thought: (At p 139)
"The law performs a critical part in anchoring educational strategies for combating bullying, but it can only go so far when dealing with minors."

Challenging Thought: (At p 150) "…many schools still do not have effective anti-bullying policies in place, and…there is a lack of awareness and resourcing in schools to manage the issue effectively."

- *CB frequently impacts on good order and management of the schools (and teachers are frequently also affected by these behaviours).*
- *How does criminal and civil law play out in the educational/ school policy environment?*

Butler, Kift, Campbell, Slee & Spears. (2011) School policy responses to cyberbullying : an Australian legal perspective. International Journal of Law and Education, 16(2), pp. 7-28. *http://eprints.qut.edu.au/49320/*

Unlike the United States, ***in Australia there has yet to be a dedicated legislative response to bullying, let alone cyberbullying****, apart from Division 8B of the Crimes Act 1900 (NSW).This section, which was inserted into the principal Act by the Crimes Amendment (School Protection) Act 2002 (NSW),makes specific criminal provision in section 60E for assault, stalking, harassment or intimidation of any school staff or student. The terms of the section are capable of embracing cyberbullying. This section is unique in the Australian criminal law, but is limited in its scope to staff and students while 'attending the school'. As such, the section will only apply in a cyberbullying context where the conduct actually occurs on the school premises or while entering or leaving school premises for the purposes of school activities.*

Schools will generally be concerned for the wellbeing of their students. School authorities will also be concerned to minimise their exposure to legal liability. Accordingly, in the context of a consideration of the adequacy of school responses to the threat of cyberbullying, the relevant laws will primarily be those laws that are capable of extending responsibility for the misbehaviour beyond the perpetrator to the school, namely negligence and defamation.

And further…

From the perspective of school authorities who seek not only to establish systems that will provide the best learning environments for their students but also to discharge their legal duty of care, lessons may be learnt from those cases of face-to-face bullying that have resulted in courts awarding compensation. Principal among those is that it is essential for schools to have effective policy documentation that addresses bullying, and by extension cyberbullying, and that those school policies are well-publicised, enforceable and implemented consistently.

Q 20: In light of the Government's proposed initiatives targeting cyberbullying set out in Chapters 1 & 2; **do the current criminal laws relating to cyberbullying require amendment**?

Response:

We do not as a general rule, support the criminalising of children. *Bullying and cyberbullying reflect child mental health-related concerns, and should be addressed so as to support young people's mental health.*

From considering the laws which can currently be employed at both State and Commonwealth level, for various behaviours associated with cyberbullying, AUARA, whilst fundamentally not supporting the use of legal sanctions in the first instance, has determined that the current laws are sufficient and do not require amendment, as they are broad enough to be able to be used in relation to specific behaviours, if required for a high level offence. The caveat to that, however, relates to the age and vulnerability/capacity of the child/young person to understand them and the penalty which accompanies them.

How would the law be useful in cases such as this, for example:

ABORIGINAL teenagers in remote communities of central Australia are using X (social media) to regularly threaten suicide, prostitute themselves and talk about substance abuse.

Child welfare advocates have sent The Australian posts from children as young as 13 that lay bare the dysfunction of the region.

Bullying is also commonplace, with teenagers regularly threatening violent abuse on the site.

http://nacchocommunique.com/2014/02/20/naccho-aboriginal-health-social-media-the-new-health-danger-in-aboriginal-communities/

As young people have also indicted in their qualitative responses, they do not think that a law would have any real impact on them, other than on perhaps increasing reporting, which they suggested would occur if there was a law specifically, but they were of the belief that it would send the behaviours underground, so some consideration of how young people view laws generally, needs to be given.

Traditionally adolescence is a time of testing boundaries, flaunting social norms and laws and exploring identity and place. This does not sit well with having a rigid legal approach to any adolescent behaviours which can be quite literally transitory and intentionally mean, but without being necessarily hostile and criminal in intent.

Rather, the preferred option, is to embark on a comprehensive information/education campaign to inform young people and their parents about the existing laws which can be applied, including that related to sexting. It would seem from young people's responses that they have an increased awareness of the laws relating to pornography, but this would need to continue to be reinforced with each new cohort, each year. An information/education campaign about the existing laws, therefore, could not be a one off event, and needs to be part of an ongoing cycle of campaigns.

The following pamphlet was produced by the SA Coalition to Decrease Bullying, Harassment and Violence in SA Schools, for parents, teachers and young people, and articulates, with the help from SAPOL, some examples of e-crime, with the relevant law noted alongside. It undergoes continual updating and review, and serves to inform the community that there are existing laws, which can be applied, under certain circumstances.

http://www.decd.sa.gov.au/docs/documents/1/CyberBullyingECrimeandthe.pdf

Become cybersmart

Get to know the resources and information available from the ACMA Cybersmart website at www.cybersmart.gov.au

Tips for children and young people

If cyber bullied:

- stay calm
- think clearly
- talk to trusted peers and adults.

Access:

- information from the websites listed in this pamphlet
- confidential counselling from the Second Story on 8232 0233 or the Kids helpline on 1800 55 1800.

Where you can get help

Your school

Keeping children and young people cybersafe is in everyone's best interest. Contact the school which your child attends. Principals can act on events beyond the school gate when student wellbeing at school is affected.

Helplines for parents and caregivers

If you need additional advice, for DECS schools contact the DECS Parent Helpline: 1800 222 696. For Catholic and independent schools, phone the school.

For confidential support, phone the ACMA Cybersafety Contact Centre on 1800 880 176 or the Children, Youth and Women's Health Services Parent Helpline on 1300 364 100.

Want to express your concern?

About an e-crime

If you think the cyber event you know about may constitute a crime (see overleaf) you can contact your local police station or BankSA Crime Stoppers on 1800 333 000. Advice is also available from the ACMA Cybersafety Contact Centre on 1800 880 176.

Produced in collaboration with the Coalition to Decrease Bullying, Harassment and Violence in South Australian Schools

Further information about the Coalition can be found at
www.decs.sa.gov.au/speced2/pages/bullying/theCoalition/

The membership of the Coalition includes representatives from the three schooling sectors and the University of South Australia, Flinders University and the University of Adelaide.

About your child accessing offensive sites

If you wish to report offensive or illegal content or online child exploitation you can complain to ACMA. At www.cybersmart.gov.au go to 'cybersafety help'. ACMA will investigate the matter for you, but will not investigate complaints about something that a person disagrees with or simply does not like.

Websites worth visiting

- Kids Helpline www.kidshelp.com.au
- Child and Youth Health www.cyh.com
- Cyberbullying Stories www.cyberbullyingstories.org.au
- DECS advice to parents and caregivers www.decs.sa.gov.au/speced2/pages/bullying/ www.decs.sa.gov.au/speced2/pages/cybersafety/
- Bullying. No way! www.bullyingnoway.com.au
- Australian Communications and Media Authority (ACMA) Cybersmart website www.cybersmart.gov.au
- ThinkUKnow internet safety program www.thinkuknow.org.au

Cyber bullying, e-crime and the protection of children and young people

Advice for families

This pamphlet provides information and advice about what to do if children or young people are feeling unsafe or uncomfortable following online or mobile phone communications, or exposure to offensive internet sites.

What is cyber bullying?

E-technology provides individuals with a powerful means of communicating instantly with others in both positive and negative ways.

Cyber bullying is bullying which uses e-technology as a means of victimising others. It is the use of an internet service or mobile technologies – such as email, chat rooms, discussion groups, instant messaging, webpages or SMS (text messaging) – with the intention of harming another person.

Examples can include communications that seek to intimidate, control, manipulate, put down or humiliate the recipient.

Activities can include repeated negative messages, sexual and racist harassment, denigration, impersonation, trickery, exclusion and cyber stalking.

Cyber bullying may involve varying levels of severity, ranging from occasional messages to frequently repeated and highly disturbing threats to a person's life.

The targeted person often feels powerless and may need help.

Cyber bullying can be an e-crime, a fact often not clearly understood by those involved.

What is e-crime (electronic crime)?

E-crime occurs when a computer or other electronic communication devices (eg mobile phones) are used to commit an offence, are targeted in an offence, or act as a storage device in an offence.

A minority of children and young people are involved in e-crime.

Examples from the South Australian Police (SAPOL)

Sexting may be an e-crime

With my mobile phone I took a photo of my girlfriend naked and sent it by text to everyone. What a laugh!

Offence: Production or dissemination of child pornography

Maximum penalty: Imprisonment for 10 years

Impersonation may be an e-crime

I got into their email account and sent abusive emails to everyone in the address book.

Offence: Unlawful operation of a computer system

Maximum penalty: Imprisonment for 6 months or $2,500

Intimidation may be an e-crime

He told me if I didn't do what he said he would but that photo on the internet and tell all my friends. I was so embarrassed.

Offence: Blackmail

Maximum penalty: Imprisonment for 15 years

Harassment may be an e-crime

I created a website about X and we all put stuff on there about how much they and everyone else like them are hated.

Offence: Racial vilification

Maximum penalty: $5,000 or imprisonment for 3 years, or both

Other offences

Using internet or mobile phone carriers:

- for suicide-related material
  Maximum penalty: $100,000
- to make a threat
  Maximum penalty: Imprisonment for 7 years
- to menace, harass or cause offence
  Maximum penalty: Imprisonment for 3 years.

What schools are doing to protect students

Research shows schools are one of the safest environments for your child. South Australian schools have been shown to have the lowest rate of school bullying compared with other states and territories (Australian Covert Bullying Prevalence Study, Edith Cowan University, March 2009). Your school will have the following safety measures in place.

Guidelines

Schools have clear guidelines about bullying. Most have user agreements or policies regarding internet access and mobile phone use. Principals use discipline procedures for breaches. A suspected e-crime or capturing a crime on a mobile device may result in SAPOL intervention.

Filters

Schools use filters to guard against students accessing inappropriate online material. However, with the explosion in wireless and mobile devices students can bypass these conventional network systems. Behaving safely online is more effective than filtering.

Training

All teachers are required to undertake Responding to Abuse and Neglect: Education and Care Training which provides guidance on keeping children and young people safe. Schools are taking up the cybersafety professional development program offered by the Australian Communications and Media Authority (ACMA). This program provides valuable information about the risks confronting students online and strategies to help make their experiences safe and positive.

Child protection programs

The Department of Education and Children's Services (DECS), Catholic Education South Australia and the Association of Independent Schools of SA are implementing child protection initiatives across South Australian schools.

Tips for parents and caregivers

Parents place boundaries on children and young people when they go beyond the front gate. We should also place boundaries on them when they leave home via the internet.

Talk to your child

Discuss how to behave to stay safe online with your child. Reassure your child that you are there to help if they get into trouble.

Provide safe and supervised access

Consider where and when your child accesses the internet and mobile technologies. It is recommended that internet access, including wireless access, should be in a public place. Mobile phones can provide internet access out of your sight. Make sure you have safety software installed – antivirus, spyware and a firewall, and age-appropriate parental controls.

Monitor e-technology use

Know what sites your child is using to talk and share online. Remind your child that their digital footprint is permanent and can be tracked by others.

Observe your child's behaviour

Watch and act upon any behavioural changes in your child.

Seek support

Use the contacts in this pamphlet if you are concerned about changes in your child's behaviour. For example, you could contact ACMA to request the removal of offensive or illegal content from a website.

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

Response:

Using a Carriage service to menace, harass or cause offence

AUARA agrees that this section of the Criminal Code can be applied to cyberbullying perpetrators. However, in a situation where the perpetrator and victims are minors, the maximum penalty of imprisonment for three years, would seem excessive, particularly for a first offence.

The role of an education campaign would be important here, to raise awareness about this law, and to find ways of couching it in more youth-friendly language: (What is a Carriage service, for example: How would young people know what that is unless it is explicitly taught to them)

Option 2: *Create a separate cyberbullying offence covering conduct where the victim is a minor (under 18 years) with a lesser maximum penalty such as a fine.*

COMMENT

AUARA does not consider that there is a need to create a separate cyberbullying offence for minors, as the existing laws, whilst created at a time when online safety was not an issue, are comprehensive enough to be applied to aspects of the behaviour when conducted online. Should the penalty for the existing laws be reconsidered, as in the previous response, then this would be sufficient.

Considerations

Why does Australia feel there is need for a specific criminal law for cyberbullying?

- Is it politically motivated? E.g. like terrorism laws? And seen as a quick fix? A get tough stance?
- Is it the digital divide and the unknown?
- Is the media linking only cyberbullying with suicide?
- Is it following other countries such as the U.S. and N.Z?

Challenging Thought
Cyberbullying and Traditional Bullying contribute to Suicidal thoughts:
Hinduja S, Patchin JW (2010). Bullying, cyberbullying and suicide: ***Archives of Suicide Research 14, 206-212, 2010***

Youth who experienced traditional bullying or cyberbullying, as either an offender or a victim, had more suicidal thoughts and were more likely to attempt suicide ***than those who had not experienced such forms of peer aggression****. Also, victimisation was more strongly related to suicidal thoughts and behaviors than offending.*

*The findings provide further evidence that adolescent peer aggression must be taken seriously both at school and at home****, and suggest that a suicide prevention and intervention component is essential within comprehensive bullying response programs implemented in schools****.*

What might be some consequences if a specific criminal law was introduced in Australia for cyberbullying?

Definitional: Academic; Survey; Legal

- There are significant difficulties in determining an academic definition for research purposes; a survey definition for community understanding purposes and a legal definition for purposes of executing the law.

***Challenging Thought*:**
Langos, C (2012) Cyberbullying: The Challenge to define. *Cyberpsychology, Behavior and Social Networking,* 15 (6), p 288 wrote:

'The reasonable person approach is an objective test that measures the conduct of the perpetrator against conduct of a hypothetical reasonable person placed in a similar position as the victim. This approach is widely adopted in both criminal law and law of torts. In Australia, it is not uncommon for offences to be defined by the reasonable person test in relation to harassment or workplace bullying. Applying the reasonable person standard to the cyberbullying context would set some boundaries to an establishing intention. It would serve as a practical tool for diminishing the level of subjectivity from a finding of intention. By introducing the reasonable person standard as an objective measurement of conduct, intention becomes a practicable element of the definition.'

Difficulties with law enforcement

- Extensive surveillance required
- Police training and resourcing
- State vs Commonwealth

Problem of Anonymity

Potential re-victimisation by justice system

Age of criminality

High standard of proof

- Evidence of intent, defence
- Consent – normal playing around

Would a specific law reduce cyberbullying?

Would it act as a deterrent?

- Young people are impulsive; do not believe they will be caught;
- Do laws on underage sex; graffiti; and drug taking stop those behaviours?

How would it affect schools?

- Would it give redress to the victims?
- Would some schools not report to police to protect their reputation?
- Will it become a social norm, a symbolic law but not enforced? – e.g. NZLRC
- Or bring the law into disrepute?

Q22: is there merit in establishing a new mid-range cyberbullying offence applying to minors

Response:

AUARA does not support the criminalising of children in Australia, so the introduction of a new, specific mid-range offence, would be an opportunity to *not* try to work across other levels of relationship restoration.

How can cyberbullying be graded so finely as to determine what is a low, medium range or high level offence?

Cyberbullying is: and it is impacting. How resilient or what coping mechanisms are available to young people in their social response repertoire is more appropriate to consider, rather than a fine, granulated approach to penalties and offences.

3.2 Options for a Commonwealth civil penalty regime

Option 3: Create a separate civil enforcement regime to deal with cyberbullying modelled on the New Zealand "Approved Agency" approach

The New Zealand Government has introduced the *Harmful Digital Communications Bill* into Parliament, November 5, 2013. This Bill proposes a new criminal offence for causing harm by posting digital communication. The Criminal Offence proposed is Option 2 above. It also provides for a civil enforcement regime, and a person complaining of being the subject of harmful digital communications may make a complaint to the "Approved Agency". In Australia this would be the Children's e-Safety Commissioner. Complaints can also be made by the parent, guardian, or school principal. If not satisfied, the complainant can go to court and seek various take-down orders.

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

Response:

Given that we already have the Online Content Scheme, as part of the *Broadcasting Services* Act, 1992, which provides a complaints-based scheme for offensive and illegal online content, with ACMA having the power to issue take-down notices, AUARA does not support the introduction of a civil enforcement regime as described. Furthermore, it considers that this complaints-based role of the Children's e-Safety Commissioner to be a time consuming waste of his/her role, and more attuned towards an Ombudsman role.

AUARA would strongly want to see the Commissioner **adopt a significant advocacy role**, rather than a complaints-based one. Furthermore, the involvement of the Commissioner in the daily dispute resolution and mediation activities, is not the best use of this highly skilled resource.

AUARA strongly argues that the Children's e-Commissioner, is **a substantive advocacy role, who would work with and across government nationally and internationally, to develop appropriate policy, in the best interests of children in this country. Investing in such a role, should not be to provide a glorified counsellor, but rather of a leader in and for children's rights, as they navigate the online social space**

Q 24: What penalties or remedies would be most appropriate for Options 2 & 3?

Option 2: Create a separate cyberbullying offence covering conduct where the victim is a minor, with a lesser maximum penalty, such as a fine.

Option 3: Create a separate civil enforcement regime to deal with cyberbullying, modelled on the New Zealand 'Approved Agency' approach.

AUARA would advocate that a panel of experts be set up, to examine the differing penalties or remedies that best support young people and their mental and physical health. This reference group would have membership from all relevant bodies: educators, social workers; psychologists, police, lawyers, and bureaucrats, including representation from ACMA, as they currently work with removing online content in conjunction with the police.

AUARA RECOMMENDATIONS

- An overview is provided of existing frameworks e.g. National Safe Schools Framework with a view to further strengthening and supporting its work in schools that directly focuses on legal issues
- A consultative panel involving young people is established and/or used to develop a national awareness campaign addressing the issue of bullying/cyberbullying
- aAcomprehensive national reviews of state and national laws addressing bullying in all forms and identify any jurisdiction issues
- Further consideration is given to 'defining' what is meant by bullying
- The Commissioner **adopt a significant advocacy role**, rather than a complaints-based one
- That a panel of experts be set up, to examine the differing penalties or remedies that best support young people and their mental and physical health.