Australian Government

Department of Communications

Regulation Impact Statement

Enhancing Online Safety for Children

November 2014

GPO Box 2154 Canberra ACT 2601 Australia • telephone 02 6271 1000 • website

Contents

Appendices

1. What is the policy problem to be solved?

The internet is a daily integrated part of life for many Australian families, providing children with a means through which they can exchange information, be entertained, socialise, do school work and conduct research.

The internet is becoming increasingly accessible for children due to the growth in ownership of internet connected mobile devices, with research indicating that 53 per cent of children own or access their first internet connected device before 10 years old;[1] and around half of 14-17 year olds access the internet through mobile phones,[2] with 43 per cent of them having their own smartphone.[3] While this increased pervasiveness of devices offers many benefits, it allows children greater capacity to access the internet 'under the radar' of parents, teachers and other supervising adults.

Use of social media services, that is use of online platforms designed to build social networks or social relations among people who share interests, activities, backgrounds or real-life connections, has also grown dramatically to overtake other forms of online entertainment and communications used by Australian children.

In 2011, the use of social media was identified as the primary form of digital communication between young people over 13, overtaking more traditional means such as text messages, phone calls and email.[4] While around half of young Australians aged between 8 and 11 years use social media services, this figure dramatically increases to around 90 per cent for 12 to 17 year olds.[5] A 2014 report indicates that 89 per cent of 12 to 17 year olds use Facebook and 65 per cent use YouTube.[6]

In this new digital environment, with more children independently accessing the internet and using social media without adult supervision, Australian children are more exposed to online safety risks, such as cyber-bullying.

While bullying itself is not a new problem, with children spending ever more of their time online, social media services and other forms of electronic communication have become a new forum for bullying and this has resulted in vastly increased opportunities and methods for bullying to occur. 'Cyber-bullying' can occur in a variety of ways, through a range of digital devices and mediums, most commonly smartphones and social media services. As many victims have pointed out, when they are physically bullied in the playground, they at least know that they are safe for a while when they get home. But if looking at a smartphone or a computer immediately exposes a victim to a stream of derision, ridicule or hatred, then they are less able to escape the bullying.

---

[1] Telstra, *Safer internet and back to school survey* (internal report), January 2013
[2] Australian Communications and Media Authority, *Like, post, share: Young Australians' experience of social media - Quantitative research report*, 2013
[3] Australian Communications and Media Authority, *Communications report 2011-12*, Commonwealth of Australia, Melbourne, 2012
[4] Australian Communications and Media Authority, *Like, post, share: Young Australians' experience of social media - Qualitative research report*, August 2011
[5] Australian Communications and Media Authority, *Click and connect: Young Australians' use of online social media – 02: Quantitative research report,* Commonwealth of Australia, 2009
[6] Australian Communications and Media Authority, *Connected parents in the cybersafety age*, February 2014

Cyber-bullying has been associated with a range of adverse implications, such as anxiety, suicidal thoughts, depression and psychosomatic and behavioural problems.[7] Research undertaken by the University of New South Wales shows a stronger association between cyber-bullying and suicidal ideation compared to 'traditional' bullying; and this is most likely due to increased exposure and humiliation, bullying episodes lasting longer and difficulties with escaping cyber-bullying.[8]

Additional information provided in a case study from the National Children's and Youth Law Centre stated that victims in the 16–17 age group reported a broad range of harms through cyber-bullying, including: feelings of embarrassment or shame; refusal/reluctance to engage in society; post-traumatic stress disorder; fear for safety; inability to continue with school; being forced to leave school and leave town; and leaving a job.[9]

Some of the more extreme cases of cyber-bullying have been associated with youth suicide. Queensland's Commissioner for Children and Young People and Child Guardian presented findings into cyber-bullying and youth suicide in May 2013 which demonstrated that cyber-bullying is one of many risk factors associated with youth suicide, with victims of cyber-bullying often possessing vulnerability characteristics known to be present in suicide deaths.

Media articles have reported the following instances where suicide deaths have been linked to cyber-bullying: in September 2013, a Tasmanian 15-year-old schoolgirl took her own life after being bullied, including cyber-bullied;[10] a 13-year-old Sydney girl took her own life in April 2013 after bullies relentlessly pursued her;[11] a 14-year-old Melbourne schoolgirl took her own life in January 2012 after suffering bullying unknown to her parents;[12] and in 2009, a Melbourne mother blamed her 14 year-old daughter's suicide on the internet.[13]

The latest data from the Australian Bureau of Statistics indicates that suicide rates in the 15-19 year old age group increased by 10 per cent from 2011 to 2012 and these numbers have been increasing since 2008.[14]

It is difficult to know the extent to which cyber-bullying influences children and young people who die due to intentional self-harm. Other risk factors are known to be relevant, including mental health problems, alcohol and drug abuse. While there is no adequate way of measuring the size of the harm from cyber-bullying in Australia, it is clear that any cyber-bullying related suicide is not acceptable to the community.

---

[7] Langos, Colette, Submission to the public consultation on *Enhancing Online Safety for Children*, 7 March 2014

[8] Spears, B., Keeley, M., Bates, S. & Katz, I (2014) *Research on youth exposure to, and management of, cyberbullying incidents in Australia: Part A - Literature review on the estimated prevalence of cyberbullying involving Australian minors (SPRC Report 9/2014)* Social Policy Research Centre, UNSW, Australia

[9] Keeley, M., Katz, I., Bates, S. & Wong, M (2014) *Research on youth exposure to, and management of, cyberbullying incidents in Australia: Part B - Cyberbullying incidents involving Australian minors, the nature of the incidents and how they are currently being dealt with (SPRC Report 10/2014)* Social Policy Research Centre, UNSW, Australia

[10] The Telegraph, *Vow to toughen cyber-bully laws as 200,000 supporters join Cassie's campaign*, 12 November 2013

[11] The Courier Mail, *13 child suicides in three years prompt call for action as bullying victims take their own lives*, 24 May 2013

[12] The Australian, *Family of suicide teen Sheniz Erkan urge parents to watch children's internet use*, 13 January 2012

[13] ABC, *Teens death highlights cyber bullying trend*, 23 July 2009

[14] Australian Bureau of Statistics, *Causes of Death, Australia*, Catalogue No. 3303.0. Belconnen, ACT: Commonwealth of Australia, 2012

The Australian Communications and Media Authority's (the ACMA) research indicates that 21 per cent of 14-15 year olds; and 16 per cent of 16-17 year olds reported being cyber-bullied.[15] Other studies indicate that 53 per cent of teens have been exposed to cyber-bullying but with only a fraction of those children choosing to tell their parents.[16] In addition, the Department of Communications released research in August 2014 which indicates that 20 per cent of 8-17 year olds in Australia were cyber-bullied in the preceding 12 months.[17]

While cyber-bullying is also an issue for adults, children are often less able to handle distressing situations such as those caused by cyber-bullying. Harmful online behaviour directed at children not only affects the parties involved, but the wider community including parents, teachers and schools.

The social media service industry provides a range of resources and tools to support and help keep users of their services safe (see Appendix A).

Despite this important work being undertaken by the social media service industry, there is no data available on the numbers of complaints made by Australian children to service providers about cyber-bullying, nor any detail available on the outcomes of any such complaints. Social media services do not publish information that enables assessment of how often they fail to respond appropriately to take down offending material. However, some qualitative evidence of major social media websites failing to respond appropriately to take down offending material has been provided via submissions to the public consultation on Enhancing Online Safety for Children, media reports and correspondence received by the Department of Communications. For example, on 27 February 2014, a report by the Law Report on ABC's Radio National featured comments from Cassie Whitehall, the sister of a cyber-bullying victim who took her own life in September 2013. Ms Whitehall claimed that a large social media service failed to remove name-calling and threatening material as it did not breach the site's community standards.

University of New South Wales research found that most cyber-bullying incidents reported occurred on social media. [18] Additionally, a case study from the National Children's and Youth Law Centre (NCYLC) stated that most cases identified either an online platform or application as the platform through which the cyber-bullying occurred. In some cases, the victim was cyber-bullied across multiple platforms.[19]

The main platforms used for cyber-bullying as identified in the NCYLC case study were Facebook (43 per cent), Snapchat (11 per cent), Ask.fm (10 per cent), Skype (5 per cent), Tumblr (4 per cent) and Kik (3 per cent).

There are a range of legal, administrative and educational initiatives currently available across all Australian jurisdictions to assist children, parents and schools with online safety concerns. However, the current range of online safety initiatives are managed and dispersed across a number of

[15] Australian Communications and Media Authority, *Like, post, share: Young Australians' experience of social media - Quantitative research report*, 2013
[16] McAfee, *Tweens, Teens and Technology* report, May 2013
[17] website
[18] Katz, I., Keeley, M., Spears, B., Taddeo, C., Swirski, T., & Bates, S (2014). *Research on youth exposure to, and management of, cyberbullying incidents in Australia: Synthesis report (SPRC Report 16/2014)*. Sydney: Social Policy Research Centre, UNSW Australia
[19] Keeley, M., Katz, I., Bates, S., & Wong, M. (2014). *Research on youth exposure to, and management of, cyberbullying incidents in Australia: Part B – Cyberbullying incidents involving Australian minors, the nature of the incidents and how they are currently being dealt with (SPRC Report 10/2014)*. Sydney: Social Policy Research Centre, UNSW Australia

agencies. This fragmentation can be confusing for the community in terms of accessing assistance for cyber-bullying issues.

A survey conducted by GfK Australia among young people aged 10-17 to find out how much they knew about the laws which apply to cyber-bullying – and what the consequences might be – indicated that there is a great deal of uncertainty and confusion about existing criminal offences related to cyber-bullying. The results suggested that while young people had an appreciation that cyber-bullying *could* be a criminal offence, there was no active on-going awareness or consideration of this issue nor a clear view of what might constitute a *criminal* case of cyber-bullying.[20]

State and territory governments are implementing a range of measures to prevent and manage cyber-bullying incidents in schools (refer to Appendix B).

Schools and local police

Research recently published by the Department of Communications found that 87 per cent of secondary schools reported at least one instance of cyber-bullying in 2013, as did just under 60 per cent of primary schools.[21]

Schools are working hard to respond to complaints about cyber-bullying, with over 83 per cent of schools having a system or policy in place for managing cyber-bullying incidents.[22] In their responses, schools typically said they had a multi-faceted approach including contacting parents, counselling of all involved parties, warning notices, class discussions, formal punishments according to school policy, and in 'extreme cases', referral to police.

Cases referred to police were more likely to involve sexting resulting from coercion, intimidation, blackmail, sharing of images or video which was unauthorised by a victim, hate websites or social media pages, and anonymous cyber-bullying.

Adding to the gap between the pervasiveness of cyber-bullying and difficulties in addressing the issue, the research found that police would typically only act on more serious cases[23] – preferring the less serious cases to be dealt with by schools or other agencies.[24] Research indicates that very few cases of cyber-bullying involving Australian minors are prosecuted. There was a preference for measures including counselling and restorative justice as the first means of redress before treating a cyber-bullying matter as a criminal offence.

These results indicate a gap between the 'extreme cases' of cyber-bullying that are unable to be dealt with adequately or effectively by schools and which are referred by schools to police, and those cases that are accepted for investigation by police because they reach a criminal threshold.

---

[20] Tan, B., and Pedic, F (2014). *Youth awareness of cyber-bullying as a criminal offence*. GfK Australia Pty Ltd

[21] *Estimates of cyber-bullying incidents dealt with by Australian schools* (2014). IRIS Research

[22] *Estimates of cyber-bullying incidents dealt with by Australian schools* (2014). IRIS Research

[23] Katz, I., Keeley, M., Spears, B., Taddeo, C., Swirski, T., & Bates, S (2014). *Research on youth exposure to, and management of, cyberbullying incidents in Australia: Synthesis report (SPRC Report 16/2014)*. Sydney: Social Policy Research Centre, UNSW Australia

[24] [24] Keeley, M., Katz, I., Bates, S., & Wong, M. (2014). *Research on youth exposure to, and management of, cyberbullying incidents in Australia: Part B – Cyberbullying incidents involving Australian minors, the nature of the incidents and how they are currently being dealt with (SPRC Report 10/2014)*. Sydney: Social Policy Research Centre, UNSW Australia

There is a great deal of uncertainty and confusion about criminal offences related to cyber-bullying and while 72 per cent of respondents to the UNSW study on youth exposure to, and management of, cyberbullying incidents in Australia considered that police would be able to do something about cyber-bullying only 36 per cent said they would report cyber-bullying to police.[25]

While there is not any specific information on the number of instances of schools failing to respond appropriately to cyber-bullying, some schools reported taking no action on cyber-bullying reports because the issue was deemed outside of the school's responsibilities; the incident did not occur during school hours; or the school chose to take no action to avoid inflaming the situation.[26]

The only avenues for redress in such situations are raising the issue with the social media service (where the cyber-bullying takes place on such a platform), or referring matters to police.

In relation to complaints made to social media services, social media services advise that they invest heavily in reporting tools and encourage their users to report any abuse, including bullying and harassment, directly to them. The social media services advise that they receive many such complaints and strive to investigate and take appropriate action promptly. However research indicates that such services have not been sufficiently responsive to requests to remove cyber-bullying material.[27] This has been reinforced by submissions to the public consultation process as well as periodic reports in the media.

While a precise number of instances where major social networking sites have failed to respond appropriately, consistent with their own terms and conditions, to take down offending material is not available, research undertaken by a research consortium led by the University of New South Wales found that fewer than half of stakeholders reporting or facilitating reports of cyber-bullying to social media services were satisfied with the outcome: "Responses from social media services that frustrated participants in this research included that material did not violate the community standards and/or that the onus was on the victim to block the bully (rather than the social media service blocking the bully)."[28]

While noting that some of the larger, more widely used social media services have significantly improved their complaints handling processes in recent years, Australian children (and their parents) currently have no recourse in instances where they disagree with how their complaints are handled by social media services.

In relation to complaints made to police, the University of New South Wales research found that the most significant barriers to police and other agencies dealing with cyber-bullying are: [29]

[25] Katz, I., Keeley, M., Spears, B., Taddeo, C., Swirski, T., & Bates, S (2014). *Research on youth exposure to, and management of, cyberbullying incidents in Australia: Synthesis report (SPRC Report 16/2014)*. Sydney: Social Policy Research Centre, UNSW Australia

[26] website

[27] website

[28] Katz, I., Keeley, M., Spears, B., Taddeo, C., Swirski, T., & Bates, S (2014). Research on youth exposure to, and management of, cyberbullying incidents in Australia: Synthesis report (SPRC Report 16/2014). Sydney: Social Policy Research Centre, UNSW Australia

[29] Katz, I., Keeley, M., Spears, B., Taddeo, C., Swirski, T., & Bates, S (2014). *Research on youth exposure to, and management of, cyberbullying incidents in Australia: Synthesis report (SPRC Report 16/2014)*. Sydney: Social Policy Research Centre, UNSW Australia

- the lack of accountability of social media and other service providers who are reluctant and/or slow to take down cyber-bullying material; and
- that many service providers are based overseas.

Further, local police have limited resources or in some instances a policing response may not be the most appropriate or most effective way of addressing the issue, particularly issues that do not warrant a criminal justice response.

In considering options for addressing these issues, the research found that respondents "clearly favoured the creation of an e-Safety Commissioner to oversee rapid take-down and act where a social network site or a cyberbully have not taken down cyberbullying content on request."[30]

It is appropriate that schools and local authorities continue to handle complaints about cyber-bullying as appropriate. The Commissioner would support and assist the ongoing activities of the schools and police in the states and territories, in addition to handling complaints that are more appropriate to be considered by the Commissioner.

Education programs

Many schools commission external providers to deliver programmes about online safety in their school. However, these programmes are not required to meet standards of quality or specifically cover cyber-bullying content. In order for educational programmes about online safety to be effective, online safety messages must be consistent and tailored to the needs of the audience.

The ACMA's Like, Post, Share Report states that 'In relation to guest speakers, almost all children and young people reported having had someone come to their schools to either talk to the whole school, year group or class. Children and young people perceptions of these talks differed largely depending on perceptions of the speaker themselves and the content that was delivered.' Speakers who were able to provide children and young people with new information, or present it in a way they had not seen before, were held as the most interesting and influential.[31]

The Department conducted a desktop review and identified over 30 different online safety programmes being delivered in schools. These programmes were found to cover a variety of online safety and security issues including cyber-bullying, online grooming and privacy. This desktop review identified a range of delivery methods including face to face presentations, video conferencing and online/desktop software.

Currently, state and territory education authorities do not have uniform requirements regarding the quality of programmes about online safety that are delivered in schools by third-party providers. There is information asymmetry in the market as principals and teachers have little guidance regarding the quality of available programmes about online safety, which can make it difficult for decision makers to assess the appropriateness of programmes to be offered within schools.

[30] Katz, I., Keeley, M., Spears, B., Taddeo, C., Swirski, T., & Bates, S (2014). *Research on youth exposure to, and management of, cyberbullying incidents in Australia: Synthesis report (SPRC Report 16/2014)*. Sydney: Social Policy Research Centre, UNSW Australia

[31] Australian Communications and Media Authority, *Like, post, share: Young Australians' experience of social media - Qualitative research report*, August 2011

There is no information available on the extent to which schools provide education on cyber-bullying that is not considered best practice.

An annual global survey of teachers' and students' internet use by AVG Technologies, released in July 2014, shows parents expect teachers to educate their children about internet safety. However, the survey's results show there is a discrepancy between parents' expectations regarding online safety education and actual time spent in class covering the topic.[32]

2. Why is government action needed?

The policy to *Enhance Online Safety for Children* is an election commitment.[33] The Government has promised to do more to protect children online.

The evidence described above demonstrates that cyber-bullying has a high prevalence amongst young people; social media services do not always adequately respond to complaints about cyber-bullying material; while schools are working hard to deal with cyber-bullying, they are unable or unwilling to deal with more complex or serious matters; and existing criminal laws are confusing and inadequate in dealing with non-criminal instances of cyber-bullying that are too complex to be adequately resolved by schools.

Even in the presence of existing penalties or other disincentives put in place by schools, governments, or others in positions of authority, cyber-bullying will still occur. Social media service providers tend to have in place policies and tools to assist users in dealing with cyber-bullying material, however when it comes to dealing with these complaints, the onus tends to be put on the victim to block the bully, and/or the victim has no recourse in instances where they disagree with how their complaints are handled by social media services. In addition, not all cyber-bullying occurs on social media.

There is a clear gap between the issues that are able to be adequately resolved by schools (e.g. those involving students within a school, or between related schools), and those that are of a criminal nature that can be dealt with by police. Such complaints would include ones that schools may consider to be outside their responsibilities (e.g. bullying occurring to one of their students by a person not at the same school), instances where the incident did not occur during school hours; and instances where the school chooses to take no action to avoid inflaming the situation.

There are existing programs in place which deliver online safety education to schools, including in relation to cyber-bullying. However not all schools, particularly those in indigenous communities or lower socio-economic areas, have the ability to pay for and offer online safety programs to their students. For these schools access to free programs such as ThinkUknow and the Australian Federal Police's HTCO Portfolio Cyber Safety Presentations are accessible.

In the absence of these issues being adequately addressed by the market or existing measures, there is a need for the Government to step in to address them. Many of the submissions to the Australian Government's public consultation supported the introduction of new measures to improve online safety for children in Australia.[34] The Government has committed to establishing the Office of the

[32] website
[33] *The Coalition's Policy to Enhance Online Safety for Children*, September 2013
[34] Public consultation was undertaken between 22 January and 7 March 2014. The Australian Government released a discussion paper entitled *Enhancing Online Safety for Children* to seek views on key online safety measures

Children's e-Safety Commissioner (the Commissioner) in the 2014-15 Budget. The Commissioner will take a national leadership role in improving online safety for Australian children by improving the coordination of messages to Australian children and those charged with their welfare and facilitating better engagement between government, families, industry and groups responsible for the wellbeing of children.

The goal of this policy is to reduce the socially undesirable behaviour of cyber-bullying of children. The policy seeks to achieve the following outcomes:

- the rapid removal of cyber-bullying material from large social media services;
- a more effective response to cyber-bullying complaints that cannot be managed at the school level but may not warrant a criminal justice response; and
- quality assurance of online safety programmes offered in schools.

The Commissioner will be responsible for achieving the above listed outcomes and implementing a range of other measures to protect Australian children online including administering a funding programme for the delivery of programmes about online safety in schools.

The lasting impacts of cyber-bullying behaviour can be significant and have long-term costs for both the individual and the wider community. The Government, alongside parents, teachers, police and social media services, has a role in ensuring children are protected online. In addition to action taken by the Government, schools will continue to play a key role in delivering online safety programs to students and in addressing the majority of cyber-bullying complaints relating to their students, and police will have an ongoing role in relation to criminal matters.

In considering the issues below, readers should note that the Government has engaged in extensive consultation with stakeholders on options to Enhance Online Safety for Children.

While in Opposition, the Coalition established the Online Safety Working Group which was chaired by the now Parliamentary Secretary to the Minister for Communications, the Hon Paul Fletcher MP. The working group consulted widely with industry, the community, parents and children — to understand the issues in keeping children safe online, and to develop policy responses. The Government's election policy to Enhance Online Safety for Children drew very heavily on the work and findings of this group.

Since coming to Government, the Government has built an even more comprehensive evidence base, commissioning three major pieces of research on cyber-bullying from research experts. The Government also consulted widely through its public consultation on Enhancing Online Safety for Children in early 2014.

The Government has committed to introduce legislation into Parliament before the end of the 2014. The Government has worked closely with key stakeholders including community groups, service providers, industry associations, business and government in the development of the legislation. The options below should be considered in this context.

3. Rapid removal of cyber-bullying material from social media services

Two policy options are considered, including:

a. status quo (non-regulatory); and

b. an effective complaints system, backed by legislation, to get harmful material down fast from large social media services:

   i. a regulatory scheme for removal of cyber-bullying material which applies to all large sites, with penalties for non-compliance; or

   ii. a two-tiered scheme, backed by legislation, for the rapid removal of cyber-bullying material from social media services.

An analysis of these options is at Appendix D. All analyses are compared relative to the status quo and to each other, rather than in absolute terms.

Of these options, (b)(ii) is considered to have the highest net benefit on the basis that it would produce a greater reduction in the amount of harm resulting from cyber-bullying than option (a), and commensurate reduction in harm when compared with option (b)(i), but would have significantly lower costs than option (b)(i).

This is summarised in the table below. The preferred option is highlighted.

Option	Harm from number of general instances*	Harm from exposure to material*	Harm from further behaviours*	Regulatory cost
Status quo	5	5	5	Low
Regulatory scheme applying to all sites	5	8	6	High
Two-tier scheme	5	8	6	Low/medium

*Harm - (1 = significant increase; 5 = no change; 10 = significant decrease/no more instances, exposure, or further behaviours).

4. Response to perpetrators of cyber-bullying

Four policy options are considered, including:

a. status quo (non-regulatory);

b. implement education and awareness raising measures to better explain the application of existing offences;

c. create a separate cyber-bullying criminal offence covering conduct where the victim is a minor, with a lesser maximum penalty; and

d. create a separate cyber-bullying notice regime to deal with cyber-bullying behaviour.

An analysis of these options is at Appendix E. All analyses are compared relative to the status quo and to each other, rather than in absolute terms.

Of these options, (d) is considered to have the highest net benefit on the basis that it would have a commensurate level of regulatory costs to the other three options, but would produce equal or greater benefits in terms of reducing harm from cyber-bullying material in comparison to the other options. Option (b) is also considered to be favourable on the basis that it would greatly reduce the harm caused from general instances of cyber-bullying, while having a very low regulatory impact.

This is summarised in the table below. The preferred options are highlighted.

Option	Harm from number of general instances*	Harm from exposure to material*	Harm from further behaviours*	Regulatory cost
Status quo	5	5	5	Low
Education and awareness raising measures	7	5	7	Low
New cyber-bullying offence	6	5	9	Low
New cyber-bullying notice regime	6	8	9	Low

*Harm - (1 = significant increase; 5 = no change; 10 = significant decrease/no more instances, exposure, or further behaviours).

5. Quality assurance of online safety programmes offered in schools

Two policy options are considered, including:

a. status quo (non-regulatory); and

b. voluntary certification process.

An analysis of these options is at Appendix F. The two options are compared relative to each other, rather than in absolute terms.

Of these options, b is considered to have the highest net benefit on the basis that, while it would involve slightly higher costs for participants than the status quo, such costs would be voluntary, and the certification of providers of program would lead to a higher reduction in harm from cyber-bullying material in comparison to option a.

This is summarised in the table below. The preferred option is highlighted.

Option	Harm from number of general instances*	Harm from exposure to material*	Harm from further behaviours*	Regulatory cost
Status quo	5	5	5	Low
Voluntary certification	7	7	7	Low/medium

*Harm - (1 = significant increase; 5 = no change; 10 = significant decrease/no more instances, exposure, or further behaviours).

6. Consultation

Full public consultation was undertaken between 22 January and 7 March 2014. The Australian Government released a discussion paper entitled *Enhancing Online Safety for Children* to seek views on implementing the key measures to improve the online safety of Australian children, including: establishing a Children's e-Safety Commissioner; developing an effective complaints system, backed by legislation, to get harmful material down fast from large social media services; and examining existing Commonwealth legislation to determine whether to create a new, simplified cyber-bullying offence.

Over 80 submissions were received from a range of stakeholders, including community organisations, industry, education bodies, government bodies, legal representatives and/or bodies, academics and individuals. Non-confidential submissions are available on the Department of Communications' website.

In addition, the Government held targeted consultation with industry and members of the OSCWG. The OSCWG was formed to enable detailed consultation on the development of online safety policies and has members drawn from community groups, internet service providers, industry associations, business and government.

A full list of OSCWG members is available here.

Consultation with the Department of Education and the ACMA has been undertaken on alignment to the National Safe Schools Framework and on approaches to implementing the voluntary certification process.

In addition, targeted consultation with education authorities, industry and members of the OSCWG will be undertaken in late 2014 / early 2015 to further assess the impact of the voluntary certification process on online safety programme providers and to align the certification criteria and guidelines to state and territory education requirements.

Further targeted consultation on the Regulatory Impact Statement has occurred with the OSCWG. A summary of the feedback received from this consultation is outlined at Appendix G.

7. What is the best option?

Following public and targeted consultation, a combination of regulatory and non-regulatory measures to address cyber-bullying is proposed.

The proposed combination of measures is set out below:

Government Actions	**Removal of cyber-bullying material from social media**	**Response to perpetrators of cyber-bullying**	**Quality assurance of online safety programmes**
Options	a. Status quo	a. Status quo	a. Status Quo
	b. Effective complaints system, backed by legislation	b. Education and awareness raising	b. Voluntary certification process
	i. Regulatory scheme applying to all participating sites	c. Separate cyber-bullying offence	
	ii. Two-tier scheme	d. Separate cyber-bullying notice regime	

By taking a holistic approach to enhancing online safety for children, there is a higher likelihood of successfully reducing the occurrence of cyber-bullying and the harm suffered by children from this

behaviour. The proposed approach aims to address issues around both the prevalence of cyber-bullying (through education and awareness raising) and its harmful effects (through education and awareness raising, and through the provision of additional remedies to address instances of cyber-bullying).

By establishing the two-tiered scheme in legislation, it will help to build the confidence and trust of Australian families in how social media services deal with their concerns.

The voluntary certification process will aim to provide quality assurance of online safety education provided in schools and enable schools to identify programmes and providers that are likely to be the most appropriate to meet the needs of their students and school community.

There is a risk that online safety programme providers may choose not to participate in the voluntary certification process or that schools are not aware of its operation. To mitigate this risk, the proposed option will involve consultation with industry, and the Commissioner will undertake information campaigns targeted at education authorities and schools to communicate the benefits of engaging certified online safety programmes. Linking the $7.5 million funding programme with the voluntary certification process will also encourage providers to certify their programmes.

Conducting the voluntary certification process may affect the ability of providers to compete in the market.

The regulatory burden and cost offset estimate for this package of options is at Appendix H.

It is difficult to monetise the benefits of reducing the consequences of cyber-bullying, whether those benefits are in the form of reduced suffering for the victim, a potential reduction in the loss of life due to self-harm or the long-term effects on family and friends, but by any measure it is self-evident that these benefits constitute a net positive benefit when compared with the average annual regulatory costs at Appendix H.

8. Implementation and evaluation

Legislation to establish the Commissioner and associated functions will be introduced in 2014. The Commissioner's Office will formally commence in mid-2015. The Commissioner will be responsible for implementing and overseeing the proposed measures.

The new arrangements would be subject to a formal evaluation from 2018 (i.e. three years after the arrangements commence). The Commissioner would monitor implementation and report on this to the Minister for Communications. An implementation plan has been developed and will be regularly reviewed and updated as needed.

8.1. Implementation risks for rapid removal of cyber-bullying material from social media services

There is potential difficulty in enforcing compliance with the legislative arrangements against large social media services which do not have an Australian presence. The design of the two-tiered scheme should reduce the circumstances in which enforcement will become an issue. In addition, a complainant also has other avenues, such as the cyber-bullying notice regime to seek redress for cyber-bullying.

The Minister will not be able to declare smaller social media services under Tier 2 (unless they volunteer to participate under Tier 2) and hence, these sites may not be subject to legally binding notices and penalties. This may result in these smaller sites not responding to requests from the Commissioner to remove cyber-bullying material.

However, the Commissioner will be expected to build strong working relationships with social media services used by children in Australia, whether formally subject to the legislation or not. The Commissioner will make informal requests to the sites not subject to Tier 2 regulation to remove cyber-bullying material – and will also highlight to them the Australian regulatory framework and the potential of the relevant social media service becoming subject to formal regulation in Australia if it becomes bigger.

8.1 Implementation risks for response to perpetrators of cyber-bullying

An implementation risk of the cyber-bullying notice regime is that the Commissioner will receive a higher number of complaints than estimated. If this occurred, the Commissioner may be overburdened by his or her workload and this could result in an additional risk that complaints may not be responded to in a timely and effective manner. To mitigate this risk, the Commissioner would focus on complaints that cannot be handled more appropriately by a school or the police and where appropriate refer complaints to relevant organisations. To reduce duplication and minimise the number of complaints handled by the Commissioner, the Commissioner will work with schools and police to establish processes to work together, undertake an information campaign to outline the purpose and role of the Commissioner and develop guidelines for handling reports of cyber-bullying.

There is a risk that the Commissioner may not be able to identify perpetrators of cyber-bullying and may therefore not be able to send a notice. This may occur in some cases despite the cooperation of social media services or other service providers. However, while the Commissioner may not be able to identify the perpetrator in all instances, notices will be useful tools for the Commissioner as they will be able to be issued in instances where the perpetrator can be identified.

8.2 Implementation risks for quality assurance of online safety programmes offered in schools

An implementation risk of the voluntary certification process is that the Commissioner will receive a higher number of applications than originally estimated. If this occurs, the Commissioner may not be able to assess applications in a timely and effective manner. To mitigate this risk, the Commissioner will work closely with online safety programme providers to manage stakeholder expectations in the event of high numbers of applications.

The Commissioner will also develop strong working relationships with industry to encourage participation in the voluntary certification process.

Appendix A

Existing online safety tools and resources provided by social media service providers

The social media service industry provides a range of resources and tools to support and help keep users of their services safe.

Social media service providers offer their services under terms of use that govern the behaviour of users of the services. For example:

- Yahoo!7's Terms of Service[35]
- Facebook's Statement of Rights and Responsibilities[36]
- Microsoft's Terms of Use[37]
- Twitter's Terms of Service[38]
- Google Terms of Service[39]

In addition, many of the services explain the standards that people must adhere to when using the services. For example, Facebook provides its Community Standards[40], YouTube provides the Community Guidelines[41] and Twitter publishes The Twitter Rules.[42]

To promote compliance with these policies, social media service providers offer tools that leverage the communities active on the sites, to flag or report instances of content or behaviour that violates these services' terms of use or community standards. For example:

- Facebook provides report links throughout its website[43]
- Yahoo!7 provides tools to assist in reporting inappropriate or harmful behaviour such as "Report Abuse" flags and Abuse Help Forms. The "Report Abuse" flags are tools that enable a user to notify the customer care teams of a complaint about specific content.
- Twitter provides a How to Report an Abusive User function[44]
- YouTube provides a flag system that enables users to report any videos which they consider to be inappropriate[45]

[35] website
[36] website
[37] website
[38] website
[39] website
[40] website
[41] website
[42] website
[43] website
[44] website
[45] website

- Microsoft allows users to report abuse[46]

Members of the Australian Interactive Media Industry Association's (AIMIA) Cyber-safety sub-group (cyber-safety sub-group), which includes Facebook, Google, Twitter, Microsoft, eBay and Yahoo!7 have advised that they maintain extensive review teams that operate continuously to take appropriate action with reports made in relation to their content or conduct on their services.[47] Complaints made to these services are triaged, with complaints dealing with the most serious cases handled first.

AIMIA cyber-safety sub-group members advise that they regularly update and improve their reporting tools. For example, Facebook last year rolled out a new tool to assist with greater transparency in identifying the status of a report made via its Support Dashboard.[48]

YouTube's 'Safety Mode' is a tool that operates at the family level and empowers parents to determine what content they wish their children to be exposed to. By switching on this tool, users have the option of choosing not to see mature content that they or their children may find offensive, even if the content does not breach YouTube's Community Guidelines. Further, YouTube videos that have been age restricted will not show up in video search, related videos, playlists, shows and movies.

In a similar manner, Microsoft provides its users with its 'Family Safety Centre'.[49]

Yahoo!7 incorporates safety and privacy features into all its products, including privacy preferences, blocking capabilities, abuse flagging and product specific FAQ safety guides[50] and general online safety tips.[51]

AIMIA cyber-safety sub-group members also provide help and educational information through specifically designed parts of their sites in order to promote awareness of their online safety policies. For example:

- The Yahoo!7 specialised safety website, which contains tools, tips, hints from experts and other information aimed at keeping children and internet users safe online.[52]
- The Google Good to Know site[53] and Safety Centre[54], which contains safety tips from experts and information about Google's online safety tools.
- eBay's Policies Centre[55] which includes information on phishing, protecting personal information and identity theft schemes[56] and Trust and Safety Tutorials.[57]

[46] website
[47] website
[48] website
[49] website
[50] website
[51] website
[52] website
[53] website
[54] website
[55] website
[56] website
[57] website

- The YouTube localised Safety Centre[58], which contains content from local partners, including the Australian Communications and Media Authority, the Australian Federal Police, Kids Helpline and the Inspire Foundation on topics that include teen safety, and harassment and bullying.
- The Facebook Family Safety Centre, which contains information for parents[59], teachers[60], and teens[61] on online safety.
- The Twitter Safety Centre[62], which includes resources and information for parents, teachers, and young people, as well as Twitter's policies, guidelines and best practices.
- Microsoft's Safety Centre[63] which gives consumers the ability to put in place family safety settings for Microsoft products[64] and provides a range of different resources and information about online security and safety.

In addition to these tools and resources, individual companies undertake their own education campaigns through initiatives such as Facebook's Be Bold Stop Bullying campaign[65], Google's Good to Know[66] initiative, eBay and PayPal's Surf between the Flags[67] initiative and Microsoft's Think U Know program with the Australian Federal Police.

All members also participate in the various awareness weeks organised by Government, such as Privacy Awareness Week, Safer Internet Day, Stay Smart Online Week and the National Day of Action against Bullying and Violence.

The AIMIA Digital Policy Group launched in December 2013 (and updated in July 2014) the Keeping Australian Safe Online[68] resource which outlines the resources provided by eBay, Yahoo!7, Google, Facebook, Microsoft and Twitter.

Members of the social media service industry also collaborate with non-profit organisations and associations including The National Association for Prevention of Child Abuse and Neglect (NAPCAN), Inspire Foundation, The Alannah and Madeline Foundation, headspace, Kids Helpline, Bravehearts and Netsafe to receive expert advice about current trends and issues with the safety of young people and to ensure that these organisations have access to relevant information about the safety policies and tools that are available to users of social media services.

In January 2013, Yahoo!7, Facebook, Microsoft and Google voluntarily signed the *Co-operative Arrangements for Complaint Handling on Social Networking Sites* (the Protocol). Yahoo!7[69], Facebook[70], Microsoft[71] and Google[72] have made self-declarations as to how they comply with the Protocol.

---

[58] website
[59] website
[60] website
[61] website
[62] website
[63] website
[64] website
[65] website
[66] website
[67] website
[68] website
[69] website
[70] website

The Protocol provides for a designated and locally based contact person at participating social networking sites that the Australian Government can contact in relation to content issues. The Protocol also provides that providers will meet with government officials on a bilateral basis every six months to discuss trends and emerging issues.

These social media service providers meet regularly with the Government and other key online safety stakeholders to discuss trends and emerging issues through the Government's Online Safety Consultative Working Group (OSCWG). This includes discussions in relation to the Government's policy to Enhance Online Safety for Children.

[71] website
[72] website

Appendix B

State and territory measures to prevent and manage cyber-bullying

State and territory governments are implementing a range of measures to prevent and manage cyber-bullying incidents in schools. Along with the measures below, the Australian Federal Police are engaged in collaborative activities with industry, the Government and sporting groups. Schools are able to access free programs through the HTCO Portfolio Cyber Safety Presentations, including ThinkUknow and a range of presentations about:

- internet safety (including ThinkUknow) presented to parents, carers and teachers aimed to raise awareness of internet safety and security issues relevant to young people; and
- cybersafety, which is delivered to primary and secondary students and encourages awareness of online safety.[73]

Victoria

- In March 2013, launched the Bully Stoppers programme which aims to help students, parents, teachers and principals to ensure schools are safe and supportive places where bullying is taken seriously and not ignored. Bully Stoppers is an online toolkit which provides interactive printable tools and resources. Interactive learning modules encourage students to discuss bullying, cyber-bullying and responsible social media use. Advice sheets are also available to help deal with face-to-face and cyber-bullying.
- The Bully Stoppers programme includes two mobile apps to promote messages and teach secondary students that there is no such thing as safe sexting.
- Offers other resources on their website for preventing, managing and handling online safety incidents such as cyber bullying.[74]
- Partnered with the Alannah and Madeline Foundation to provide funding through to the middle of 2015, so all Victorian government schools and selected non-government schools can participate in the eSmart Schools online safety framework.

Queensland

- Provides advice and support to schools on online safety issues through their website.[75]
- Developed tailored programmes to help students understand what they should and shouldn't do online. [76]
- Partnered with the Alannah and Madeline Foundation to offer the eSmart Schools online safety framework to Queensland state schools.

[73] website
[74] website
[75] website
[76] website

Western Australia

- Provides links to resources, information and cyber-bullying webinars on the safe use of technology communications in the school, community and home.[77]

New South Wales

- Provides the Digital Citizenship Resource which includes a variety of games and activities to educate students on how to be responsible digital citizens.[78]
- Provides advice and tips for parents on a wide range of issues affecting children and youth at the Schools A to Z website. [79]

South Australia

- Provides advice on dealing with online safety issues through their website.[80]
- Developed resources about implementing online safety into the curriculum and links to third party resources such as the Cybersmart website.
- Offers a variety of policies and procedures for schools to take when an online safety incident has occurred.
- In December 2013, provided the Carly Ryan Foundation a $50,000 grant to develop a mobile phone app that will allow young people to communicate instantly with their carers and loved ones anytime they feel threatened, unsafe or intimidated.

Australian Capital Territory

- The Parent Link Website provides information about cyber safety issues, tips on how to stay safe online and links to various online safety resources.[81]

Northern Territory

- Provides advice for schools and families about online safety issues on their website.[82]

[77] website
[78] website
[79] website
[80] website
[81] website
[82] website

Appendix C

Overseas approaches to cyber-bullying

The Department commissioned research earlier this year into youth exposure to, and management of, cyber-bullying incidents in Australia. The research contained an evidence-based assessment of deterrents to youth cyber-bullying and part of this assessment examined what is being done in the wider international community.[83]

This research suggests that there is no standard approach that is common across each of the jurisdictions which were examined. Variations occur with regard to age of criminal responsibility, the legal response to bullying in general as opposed to specific mention of cyber-bullying, the responsibility and legal requirements for schools, and whether federal or state laws are used to address bullying and cyber-bullying (where applicable). A brief summary for each of the jurisdictions examined as part of this research follows.

US and Canada

All laws relating to cyber-bullying in the US are at the state level. Of the 49 states that have bullying laws:

- 19 include cyber-bullying specifically;
- 4 states have proposed cyber-bullying laws;
- 48 states included some form of harassment; and
- 14 states had criminal sanctions for bullying or cyber-bullying, with 5 states having criminal sanctions proposed.

No evaluations have been conducted on the impact of these laws. However, legislation without support for education campaigns and resources in schools was found to be counterproductive in the US.

Whilst there are currently no bullying laws at the federal level, a Bill was introduced into US Congress in 2009, *the Megan Meier Cyberbullying Prevention Act*, which is still under review.

In Canada, cyber-bullying can be dealt with under civil and criminal law depending upon the situation. Several provinces and territories have laws specifically dealing with online and offline bullying. Amendments to the Education Acts have been used rather than criminal law provisions.

European Union

There is no European Union legal framework regarding violence in schools; however, in several Member States there are laws that may be used to deal with specific forms of bullying.

A self-regulatory charter titled *Safer Social Networking Principles for the EU* (SSNPs) has been developed by the European Commission and Social Network Providers following public consultation on online social networking by the European Commission (European Social Networking Task Force, 2009).

[83] website

The UK has no specific law that makes cyber-bullying illegal and no legal definition of cyber-bullying; however, there are a number of existing criminal and civil laws that can be applied to cases of cyber-bullying in terms of harassing, menacing and threatening communications. There is a legal requirement for all schools to have an anti-bullying policy. In addition, schools in the UK have the power to regulate the conduct of students outside of school grounds where it affects life in school. The age of criminal responsibility starts at the age of 10.

In Belgium, a number of existing legislative provisions can be applicable to cases of cyber bullying on social networking sites: 'most are formulated in a technology-neutral manner, which implies that they may be applied in a social networking site environment'. The *Youth Protection Act* does impose, instead of the punishments of the Criminal Code, other measures, including supervision, education, disciplinary measures, guidance, advice or support, which can be imposed on parents or on the minors themselves. The age of the minor in question is considered: different measures are imposed before and after the age of 12. In addition, a Judge may give preference to victim offender mediation. Parents and teachers may in certain circumstances be held liable for the acts of their children or pupils.

In the Netherlands**,** the government is planning to have legislation on bullying in which they intend to include an obligation for schools to deal with bullying problems by, e.g. having effective anti-bullying programs in place.

In Portugal, there are no specific legal actions against bullying/school violence outside the general law about children and youth.

In Ireland, there is no legislation that expressly deals with the issue of cyber-bullying. There are a number of criminal law and education law provisions and guidelines given to schools, which implicitly include these behaviours.

Australia and New Zealand

In Australia**,** the *UN Convention of the Rights of the Child* (UNCRC) enshrines in international law that children have the same rights as adults, while also having the right to special care and assistance due to their vulnerability. A number of Australian civil and criminal laws are relevant to cyber-bullying including:

- the duty of care of schools
- crime compensation schemes
- communications law
- criminal proceedings

Police in every Australian jurisdiction have discretion to use diversionary methods for juvenile offenders in preference to using criminal proceedings. These include:

- assistance
- warnings
- cautions
- youth justice conferencing

Criminal proceedings are only used in the most serious cases or when a young person prefers to go to court. Very few such prosecutions have occurred.

The New Zealand Government introduced the *Harmful Digital Communications* Bill in November 2013. The Bill was referred to the Justice and Electoral Select Committee for consideration; the Committee's report was released on 27 May 2014. The Bill paves the way to amend and clarify existing legislation regarding digital communications, create new criminal offences to deal with the most serious acts, and create a new civil enforcement regime to deal effectively and quickly with harmful digital communications.

In establishing the offence of causing harm by posting a digital communication, the Bill provides that a person found to have committed this offence is liable to imprisonment for up to 3 months, or a fine not exceeding NZ$2,000. Within the civil enforcement regime, individuals may make initial complaints about harmful digital communications to an Approved Agency. There is no specific mention of an information and education campaign to accompany the introduction and implementation of the new legislation.

In summary, the majority of the jurisdictions examined in this research can be assigned to one of two categories:

- those that have explicit laws on cyber-bullying, and
- those who do not have specific cyber-bullying laws but have a number of existing legislative provisions or other measures, including education, support, and disciplinary actions that may be applied to cases of cyber-bullying.

A number of jurisdictions have more than one solution to address the issue of cyber-bullying and many are currently building their own evidence-base to inform future directions in this field.

Appendix D

Rapid removal of cyber-bullying material from social media services – policy options and analysis

The market has failed to adequately address all cases of harmful online behaviour targeted at children.

Research commissioned by the Government indicates that social media services have not been sufficiently responsive to requests to remove cyber-bullying material. This has been reinforced by submissions to the public consultation process as well as periodic reports in the media.

Academic commentators have expressed the view that the occurrence of cyber-bullying is not adequately addressed by current measures: 'It is clear that social networking sites…. have not done enough to protect Australian children from cyberbullying… Parents or guardians should be afforded the opportunity to take actions to protect their child from harm.'[84]

Implementing a rapid removal scheme may further assist large social media services with identifying which instances of harmful material require urgent removal, in cases where requests for the removal of harmful material have been reported but not actioned. Social media sites and end-users can be expected to benefit significantly by being able to rely upon a proper investigation by an independent authority into the circumstances of particular cases.

On 17 September 2014, the Government announced that it will implement its election commitment to appoint a Children's e-Safety Commissioner and that it was preparing legislation to enhance online safety for children to be introduced in Parliament by the end of 2014. On 28 October 2014, the Parliamentary Secretary to the Minister for Communications announced that the Commissioner would be established as an ongoing, independent statutory office within the Australian Communications and Media Authority. The Commissioner's office will be a single point of contact for online safety issues for industry, Australian children and those charged with their welfare. The Commissioner will take the lead in developing and implementing online safety policies for children, and will be responsible for the improved coordination of content and messages around online safety.

All existing online safety initiatives in the Department of Communications and the ACMA will be transferred to the Commissioner.

To give effect to the Government's commitment to have an effective complaints system, backed by legislation, to get cyberbullying material targeted at an Australian child down quickly from large social media sites, the legislation will provide for a two tier scheme, administered by the Commissioner, to deal with complaints about cyber-bullying material.

[84] Srivastava, Gamble & Boey, *Cyberbullying in Australia: Clarifying the Problem, Considering the Solutions*, International Journal of Children's Rights 21 (2013) 25-45, May 2013

What are the policy options?

Two policy options are discussed below, including:

c. status quo (non-regulatory); and

d. an effective complaints system, backed by legislation, to get harmful material down fast from large social media services:

i. a regulatory scheme for removal of cyber-bullying material which applies to all large sites, with penalties for non-compliance; or

ii. a two-tiered scheme, backed by legislation, for the rapid removal of cyber-bullying material from social media services.

a. Status quo (Non-regulatory)

Every social media service has different terms of use that govern its relationship with users who interact with the site. Most of the major social media services have terms and conditions which sufficiently prohibit cyber-bullying material. For example:

- the Facebook Community Standards prohibit "bullying and harassment";
- the Twitter Rules do not allow users to "engage in targeted abuse or harassment"; and
- The YouTube Community guidelines state that there is "zero tolerance for predatory behaviour, stalking, threats, harassment…".

The *Cooperative Arrangement for Complaints Handling on Social Networking Sites* described in Appendix A assists in improving the information that signatory social networking sites make available to their users about their handling of complaints for material posted online, and to highlight and educate social networking site users on mechanisms to deal with problems which arise on their sites.

While the Protocol is a good start, it has its shortcomings, including:

- it includes no tangible timeframes for removal of cyber-bullying material;
- compliance with the Protocol by industry is voluntary – signatories can choose to stop participating;
- it is not reviewable – no independent third party to review decisions where there is disagreement; and
- it is not enforceable – there are no sanctions for non-compliance.

b. An effective complaints system, backed by legislation, to get harmful material down fast from large social media services

In its election commitment, the Government stated that it would introduce an effective complaints system, backed by legislation, to get harmful material down fast from large social media services (the scheme). This commitment resulted from the Coalition's consultation with the community while

in Opposition, which indicated a need to have online material that is harmful to a specific child removed as quickly as possible.

i. Regulatory scheme for removal of cyber-bullying material which applies to all large social media services, with penalties for failing to comply

Features of this option include:

- The scheme would apply to all large social media services.
- A company which operates a large social media service would be required to put in place an acceptable complaints handling and rapid removal arrangement where this did not presently exist.
- The Commissioner would determine the criteria for such an arrangement and would be authorised to assess acceptability.
- In circumstances where the Commissioner finds that the complaints handling policy of a large social media service does not meet an acceptable standard, the Commissioner could issue an improvement notice.
- If the large social media service fails to respond adequately to the improvement notice, the Commissioner would be empowered to make a public statement on the shortcomings of the site's complaints handling processes.
- The Commissioner would be able to receive complaints about harmful material that is directed at a specific child from eligible complainants.
- The scheme would require eligible complainants to report and request removal of the harmful material, in the first instance, to the large social media service via the social media service's own complaints handling system, before lodging a complaint with the Commissioner.
- Where the large social media service fails to adequately respond to the complaint or fails to remove the material, the Commissioner would investigate the complaint and assess whether the material is targeted at and likely to cause harm to an Australian child.
- The Commissioner would issue a notice to remove the material to the large social media service.
- Where a large social media service or an individual fails to comply with a notice to remove material, sanctions for non-compliance would apply.

At any stage during this process, the Commissioner would be empowered to refer complaints to appropriate bodies if necessary, including police, schools and child welfare organisations.

Impacts on stakeholders

This option would impose costs on all large social media services. Costs involved would include:

- Development of appropriate systems and processes relating to complaints handling and rapid removal of cyber-bullying material, where these processes did not already exist;
- Provision of a contact person to liaise with the Commissioner on complaints referred by the Commissioner;

- Compliance with a removal notice.

The benefits of this scheme would apply to children who have been the target of cyber-bullying material. Benefits would include having cyber-bullying material taken down quickly, particularly in instances where the social media site had refused to remove material, based on its consideration of the material.

While child protection organisations and education bodies have advocated strongly for a scheme for the rapid removal of harmful material from social media services, industry is opposed to a scheme that involves heavy handed regulation.

ii. A two-tiered scheme, backed by legislation, for the rapid removal of cyber-bullying material from social media services

Following public consultation and specific negotiation with industry, a two-tiered scheme is proposed. Under this option, the Australian Government would expect that all social media services accessible to Australian children, as a matter of good practice, have a complaints management system, terms of use which sufficiently prohibit cyber-bullying material and a contact point for the Commissioner to refer complaints that users consider have not been adequately dealt with.

Legislation would set out a two-tiered scheme for the rapid removal of cyber-bullying material from social media services. Social media services voluntarily participating under Tier 1 (Tier 1 SMS) would not be subject to legally binding notices or penalties. Social media services that are declared by the Minister for Communications (the Minister) under Tier 2 (Tier 2 SMS) would be subject to legally binding notices and penalties.

Only large social media services could be declared as subject to Tier 2 regulation (unless smaller social media services volunteer to participate under Tier 2). To avoid being subject to such formal regulation, it is expected such sites would voluntarily participate in Tier 1. The legislation would state that a site cannot be subject to Tier 2 regulation while it is participating under Tier 1.

To participate in Tier 1 a site would need to lodge a written application and have it accepted by the Commissioner. The application must demonstrate that the social media service has a complaints management system, terms of use which sufficiently prohibit cyber-bullying material and a contact point for the Commissioner to refer complaints that users consider have not been adequately dealt with.

It would be open to smaller sites to voluntarily participate in either Tier 1 or Tier 2. It is expected that some sites may choose to participate in the scheme for reputational reasons.

An additional benefit of participating in Tier 1, as opposed to Tier 2, is allowing each Tier 1 site the option of having any assessment by the Commissioner of whether particular material is cyber-bullying material made by reference to the social media service's own terms of use, rather than by reference to the definition of targeted cyber-bullying material in the Act.

The Commissioner would have the power to revoke a declaration of a social media service's Tier 1 SMS status if the Tier 1 SMS repeatedly failed to act to remove cyber-bullying material following requests from the Commissioner over a period of 12 months.

The Minister could declare a site a Tier 2 SMS following a recommendation from the Commissioner.

A social media service may be declared a Tier 2 SMS, if both of the following conditions are met:

- the Commissioner is of the opinion that the social media service is a large social media service; and
- the social media service is not a Tier 1 SMS and has had reasonable opportunity to be a Tier 1 SMS; or
- the social media service has made a written application to be subject to formal regulation under Tier 2.

A social media service subject to Tier 2 would be legally required to comply with a notice to remove cyber-bullying material issued by the Commissioner. Court action can be taken where a social media service fails to comply with a notice.

The Tier 2 provisions are restricted to large social media services (except in circumstances where a site has applied of its own volition to be subject to formal regulation) to capture those sites that Australian children and young people are most likely to be using.

In addition, large sites can be expected to comply with an Australian regulatory scheme for legal and corporate reputational reasons. By contrast, smaller social media services, typically hosted, and controlled from, outside Australia, in practical terms are likely to be able to disregard Australian legislation with effective impunity. Further, this approach amounts to a formal statement of expectations on behalf of the Australian community that these are the standards that all social media services are expected to meet.

The Commissioner would receive complaints by or on behalf of Australian children regarding cyber-bullying material occurring on social media services. At any stage, the Commissioner would be empowered to refer complaints to appropriate bodies if necessary, including police, schools and child welfare organisations.

Impacts on stakeholders

This option would impose costs on participating social media services. Costs involved would include:

- Application to the Commissioner to participate in tier 1
- Provision of a contact person to liaise with the Commissioner on complaints referred by the Commissioner.

Key differences between this option and sub-option (b)(i) is the lack of costs associated with having to develop complaints handling and rapid removal systems and processes, and lack of costs associated with compliance with removal notices. Sites with pre-existing complaints handling processes would be expected to be successful in applying for tier 1 status, and would therefore not be subject to any compliance costs. As a result, it is also expected that no large sites would be declared as a tier 2 social media service.

The benefits of this scheme would apply to children who have been the target of cyber-bullying material. Benefits would include having cyber-bullying material taken down quickly, particularly in instances where the social media site had not removed material, based on its consideration of the material.

Concerns have been raised by social media sites that a rapid removal scheme may result in an increase in the volume of reports being made to social media services. However, social media sites have advised that they invest heavily in reporting tools and encourage their users to report any abuse, including bullying and harassment, directly to them. Given the extent of investment in these tools and the heavy promotion of these by sites, it is not clear that the establishment of the Commissioner would result in complaints being made that are not already being raised with the sites. Further, social media sites have not provided any evidence to back their claim that complaint volumes will increase. As a result, it is not expected that there would be any costs flowing from a rise in complaints, and if there was any rise, it would be expected to be relatively modest.

What is the likely net benefit of each option?

The harms of cyber-bullying to individuals and to society are difficult to quantify and measure. Harms associated with cyber-bullying include anxiety, suicidal thoughts, depression and psychosomatic and behavioural problems. These harms can flow on to, and impact on, other areas of life: ability to socialise, self-esteem, self-worth. It is difficult to measure how cyber-bullying occasioned as a child may impact on an individual's ability to contribute to society, enter into meaningful relationships, to find meaningful employment, etc. later in life. The flow on effects to society, including the need for provision of counselling services, provision of mental health services, assistance in seeking employment are likewise difficult to gauge.

Rather than a strict assessment of economic cost for each option (in terms of cyber-bullying harm) in determining the net benefits of each option below, regard will be given to how each option rates relative to the others against a set of pre-determined priorities which would reduce the amount of harm caused by cyber-bullying.

The priorities that each option will be assessed against are:

- ability of the measure to reduce the number of cyber-bullying instances in general (general instances of cyber-bullying);
- ability of the measure to reduce the amount of time that instances of cyber-bullying material would be available (on the assumption that the longer instances of cyber-bullying are available, and the longer they are able to be viewed or disseminated, the more harm is caused by that material) (exposure to material);
- ability of the measure to reduce further instances of cyber-bullying by the same perpetrator (further behaviours by bully).

Each option will be given a score out of 10 for each priority, with a score of five indicating no change at all (compared to status quo), and a score of 10 indicating complete absence of any general instances of cyber-bullying material, little to no exposure to material (ie taken down or removed within minutes), and no further cyber-bullying behaviours at all by the bully). A score of one would represent a significant increase in these.

Regulatory cost will be given a score of either 'low', 'medium' or 'high', relative to each other option considered.

a. Status quo (Non-regulatory)

Maintaining the status quo is the least resource intensive option.

However, it was clear from the Coalition's consultation, while in Opposition, that many parents and teachers feel ill-equipped to deal with the challenge of protecting children from online dangers. In particular, the issue of not being able to quickly remove cyber-bullying material from social media services is a significant issue. The Protocol relies upon voluntary participation of social networking sites. There are no sanctions or legal consequences for failure to comply, which lowers the incentive for a social networking site to comply with its commitment under the arrangement.

Under the Protocol, participating social networking sites have no obligation to deal with complaints or remove material within a specific timeframe. The National Children's and Youth Law Centre has indicated to the Department of Communications that:

> To delay the removal of harmful content […] is to delay crucial intervention for Australian children and young people suffering from cyber bullying, incitement to harm or suicide or the non-consensual distribution of sexually charged material. The consequences of this denial of protection can, in some cases, be catastrophic.

Further, under existing arrangements, victims of cyber-bullying cannot escalate complaints which are not sufficiently dealt with by social networking sites. The Commissioner would be a high profile, centralised point to which victims can seek redress.

The Government has made an election commitment to do more to protect children online.

	General instances	Exposure to material	Further behaviours
Harm*	5	5	5

Regulatory cost	Low (compared to other options) – no new regulation or requirements

*Harm - (1 = significant increase; 5 = no change; 10 = significant decrease/no more instances, exposure, or further behaviours).

b. An effective complaints system, backed by legislation, to get harmful material down fast from large social media services

i. Regulatory scheme for removal of cyber-bullying material which applies to all participating large social media services, with penalties for failing to comply

This option would affect all large social media services.

While the Minister for Communications would determine which social media services are considered 'large', it is anticipated that the scheme would likely apply to the social media services most used by Australian children. Most of the larger social media services are members of the Australian Interactive Media Industry Association.

It is estimated that large social media services would incur significant costs under this option, including development of appropriate complaints handling systems and processes where these processes did not already exist, provision of a contact person to liaise with the Commissioner on complaints referred by the Commissioner, and complying with orders from the Commissioner.

This option would provide a mechanism for victims of cyber-bullying to have cyber-bullying material removed where the market fails to do so. It would provide recourse for victims without victims having to seek redress through the criminal justice system.

However, consultation with industry has indicated that this option would place a heavy regulatory burden on large social media services, many of which already have well established complaints handling systems, and not impose obligations on smaller sites which may not have mechanisms for addressing cyber-bullying.

	General instances	Exposure to material	Further behaviours
Harm*	5	8	6

Regulatory cost	High (compared to other options) – all large social media services providing services to Australian children would be subject to strict regulatory measures for the removal of cyber-bullying material

*Harm - (1 = significant increase; 5 = no change; 10 = significant decrease/no more instances, exposure, or further behaviours).

ii. A two-tiered scheme, backed by legislation, for the rapid removal of cyber-bullying material from social media services

This option would affect social media services.

It is estimated that social media services would incur costs relating to:

- applying to the Commissioner to become a Tier 1 SMS; and
- providing a contact person for the Commissioner to engage with.

There would not be regulatory costs associated with complying with notices, as tier 1 sites are not subject to enforceable obligations and we expect no large sites would be declared tier 2.

The Australian Government would expect that all social media services, as a matter of good practice, have a complaints management system, terms of use which sufficiently prohibit cyber-bullying material and a contact point for the Commissioner to refer complaints that users consider have not been adequately dealt with. The majority of large social media services, predominantly used by Australian children, would reasonably be regarded to have such systems and measures in place and would be expected to fall within the non-regulatory part of the scheme (Tier 1). As a result, it is estimated that such sites would not incur costs relating to Tier 2. Further, as current business practices of such services involve maintaining a robust reporting infrastructure, regardless of

legislative requirements, and as Tier 1 SMS will not have a legal obligation to comply with requests made by the Commissioner, this proposal is not expected to place any additional costs on Tier 1 SMS other than those mentioned above.

The implementation of this option would enable the Commissioner to work collaboratively with industry and leverage social media services' existing complaints handling processes and online safety initiatives.

Design of this option reflects discussion with social media services to minimise the impact on their businesses.

The Department has consulted with stakeholders on the assumptions underpinning the regulatory costing of this option. Further detail on the feedback received is outlined at Appendix G. In estimating the regulatory impact of this option on industry, the Department has assumed that ten social media sites will apply to the Commissioner to become a Tier 1 SMS. The Department has consulted with the social media service industry, and expects that the application process will involve three employees and will involve up to five hours of work for each person. Each Tier 1 site would need to provide a contact person for engaging with the Commissioner, and it is assumed that each contact person will engage with the Commissioner up to a total of 24 days (192 hours) per year. It is also assumed that there will be no sites declared Tier 2 under the scheme, as the majority of large social media services that provide services to Australian children have business practices in place including terms of use dealing with cyber-bullying, and would successfully be able to apply for Tier 1 status under the scheme.

The two-tiered scheme would provide most of the same benefits as option (b)(i) but without placing the same regulatory burden on industry. Public-private partnership models have been successfully adopted in the United States, Europe and in the United Kingdom.[85]

This option provides a low regulatory burden for industry whilst still offering real, tangible and meaningful benefits for children who are victims of cyber-bullying, their parents and teachers. It would also deliver social benefits by reducing the harm caused by cyber-bullying on children.

	General instances	Exposure to material	Further behaviours
Harm*	5	8	6

Regulatory cost	Low/medium (compared to other options) –this option is light touch and would rely on social media services existing systems and processes. Only services in Tier 2 would be subject to strict regulatory measures for the removal of cyber-bullying material, however it is not anticipated there will be many Tier 2 services, if any at all. There would be limited compliance costs for industry, involving applying for Tier 1, and a contact person for each Tier 1 service interacting with the Commissioner on an occasional basis (up to 24 days per year), based on industry estimates.

[85] Facebook, submission to the public consultation on *Enhancing Online Safety for Children*, 7 March 2014

*Harm - (1 = significant increase; 5 = no change; 10 = significant decrease/no more instances, exposure, or further behaviours).

Of the options identified above, option (b)(ii) is considered to have the highest net benefit on the basis that it would produce greater benefits than option (a), commensurate benefits with option (b)(i), but would have significantly lower costs than option (b)(i) (commensurate with the costs of option (a)).

This is summarised in the table below. The preferred option is highlighted.

Option	Harm from number of general instances*	Harm from exposure to material*	Harm from further behaviours*	Regulatory cost
Status quo	5	5	5	Low
Regulatory scheme applying to all sites	5	8	6	High
Two-tier scheme	5	8	6	Low/medium

*Harm - (1 = significant increase; 5 = no change; 10 = significant decrease/no more instances, exposure, or further behaviours).

Appendix E

Response to perpetrators of cyber-bullying

Currently, Australian children who are the target of cyber-bullying do not have a path to seek redress against the author of the cyber-bullying material other than resorting to existing criminal law remedies.

There is limited quantitative information about how many schools fail to respond appropriately to cyber-bullying. However, schools have reported taking no action on cyber-bullying reports because: [86]

- the issue was deemed outside of the school's responsibilities;
- the incident did not occur during school hours; and
- the school chose to take no action to avoid inflaming the situation.

Cyber-bullying complaints that cannot be dealt with at the school level are generally directed to local police, who may need to manage resources in order to respond to cyber-bullying complaints. It should be noted that the police can only deal with criminal cases of cyber-bullying and are not able to act on instances that do not constitute criminal conduct.

Research indicates there is a considerable discrepancy between the number of cyber-bullying instances schools and victims of cyber-bullying say they report to police and the number of reports registered by police. Research indicates that very few cases of cyber-bullying involving Australian minors are prosecuted. It should be noted that not all cyber-bullying is, nor should be, considered criminal in nature. In addition, parents of the victim may not wish to pursue charges against the perpetrator so as to avoid their child having to go through court proceedings. Police understandably avoid investigating low level matters where the offender is a juvenile and prefer youth cyber-bullying matters to be dealt with by schools or other agencies outside the criminal justice system. This way the perpetrator may receive education and assistance to overcome their behaviours, without having a criminal record. This situation is likely to be contributing to a perception that cyber-bullying is not currently adequately addressed nor does it carry any consequences for the perpetrator.

A majority of submissions to the public consultation supported non-custodial penalties for minors, such as mediation, infringement notices and educative options.

Current arrangements to respond to cyber-bullying are ineffective, as parents and children must make a complaint to police or schools who may not be resourced or have the capability to deal with an issue effectively. The Commissioner would be a leading, high-profile figure who is easily accessible by children, parents and schools. The Commissioner's website would have an online complaints form which would be easy to fill out and appropriate for children. The staff of the Commissioner would be trained to deal with children and would have strong knowledge of the existing laws relating to cyber-bullying. The availability of a mechanism for dealing with those complaints that cannot be addressed by schools but which are not of a serious enough nature to be considered by police would address a critical gap in existing ways of addressing cyber-bullying.

[86] website

In this regard, a further element of the framework announced by the Government in October will be a power for the Commissioner to issue a notice against a person who has posted cyberbullying material targeted at an Australian child.

This notice, an 'end user notice', will for example require the end user who posted the material to remove it; to refrain from posting more such material; or to apologise to the victim.

The Government has drawn on a number of models in developing this mechanism. One is the provisions in the planned New Zealand legislation dealing with cyberbullying. Another is the experience of the National Children's & Youth Law Centre based at the University of New South Wales. They have found that in many cases a formal written request to cease cyber-bullying behaviour, issued by their service, resolves the issue.

The legislation will not include the power for the Commissioner to fine end users who fail to respond to a notice, because the Government is wary of imposing fines on children. Rather, the next steps available to the Commissioner, if the recipient of the notice fails to respond, will include going to court to seek an injunction; and referring the matter to the police.

What are the policy options?

Four policy options are discussed below, including:

e. status quo (non-regulatory);

f. implement education and awareness raising measures to better explain the application of existing offences;

g. create a separate cyber-bullying criminal offence covering conduct where the victim is a minor, with a lesser maximum penalty; and

h. create a separate cyber-bullying notice regime to deal with cyber-bullying behaviour.

c. Status quo (Non-regulatory)

The following measures and initiatives are currently available to Australians dealing with online safety concerns:

- Section 474.17 of the Criminal Code Act 1995 (Cth) (the Criminal Code) makes it an offence for a person to use a carriage service, including the internet, social media services or a telephone, in a way that reasonable persons would regard as being menacing, harassing or offensive. The maximum penalty for this offence is three years imprisonment and/or a fine of up to $30,600.

- Section 474.15 of the Criminal Code also makes it an offence to use a carriage service to threaten to kill (punishable by ten years imprisonment) or cause serious harm to (punishable by seven years imprisonment) a person. It is required that the person who makes the threat must intend the recipient of the threat to fear that the threat will be carried out.

- Each state and territory has anti-stalking and threatening behaviour laws, which may apply to cyber-bullying conduct. States and territories also have their own defamation laws which may apply to online content.

- Issues relating to online content can be the basis for complaints to the Australian Human Rights Commission under federal anti-discrimination law (for example, online content that is alleged to constitute sexual harassment or racial vilification).

- The Online Content Scheme is set out in the *Broadcasting Services Act 1992* and regulates illegal and offensive online content in Australia with reference to the National Classification Scheme.

- Existing Australian Government online safety initiatives include the Cybersmart programme, Cybersafety Help Button and Easy Guide to Socialising Online.

Commentary on the existing offences (sections 474.15 and 474.17) has suggested that the language of these provisions is difficult to understand, and as noted in the policy to *Enhance Online Safety for Children*, most people would not know what 'using a carriage service' means.

d. Implement education and awareness raising measures to better explain the application of the current offence

This option would involve providing better education and messaging to students, parents, teachers and law enforcement agencies about the current offences and the legal consequences of cyber-bullying.

Impacts on stakeholders

This option would not impose any regulatory costs on stakeholders. However students, parents, teachers and others would benefit from a greater understanding of existing cyber-bullying offences and consequences, and this would be likely to lead to reduced instances of cyber-bullying.

e. Create a separate cyber-bullying offence covering conduct where the victim is a minor, with a lesser maximum penalty

In the policy to *Enhance Online Safety for Children*, the Government committed to examining existing Commonwealth legislation to determine whether to create a new, simplified cyber-bullying offence.

A new cyber-bullying offence could be introduced to specifically address conduct where a victim is a minor, with a lower maximum penalty prescribed. Such an offence could be based on section 474.17 of the Criminal Code and would still allow recourse to the existing offence for particularly serious incidents.

Lesser penalties could include fines, counselling, restorative justice, community-based orders and probation.

Awareness raising for such a new offence would need to be undertaken, or there would be the risk that the new offence would be lost with the lack of awareness of existing offences.

Impacts on stakeholders

This option would not result in any new regulatory costs. However the introduction of a specific offence that captures less serious instances of cyber-bullying, which might be better managed by schools or parents, would cause an increase in the criminalisation of young people for objectively less serious offences.

f. Create a separate cyber-bullying notice regime to deal with cyberbullying behaviour

This option is based on the civil enforcement regime proposed in New Zealand's *Harmful Digital Communications Bill*. Under the proposed New Zealand regime, a person subject to harmful digital communication may make a complaint to an 'Approved Agency'.

A cyber-bullying notice regime would offer an Australian child who is the target of cyber-bullying material, a path to seek redress against the person who posted the cyber-bullying material. The Commissioner would be expected to engage with the relevant parties and use advice and persuasion (as appropriate) to resolve cyber-bullying complaints.

The Commissioner will assist in resolving cyber-bullying disputes involving children that take place via electronic communications and cannot be resolved at the school level but do not warrant police involvement. Cyber-bullying involving students at the same school will be best resolved by the school at first instance. Cyber-bullying involving serious threats, blackmail or other serious criminal activity would be referred to the police.

Under the regime, the Commissioner would have the power to issue a notice against a person who posted cyber-bullying material targeted at an Australian child, requiring the person to: remove the cyber-bullying material; cease posting cyber-bullying material targeted at the child and/or apologise.

If a person fails to comply with the Commissioner's notice, the Commissioner may apply to the Federal Circuit Court of Australia for an injunction against the person and/or notify Federal, State or Territory Police that the person has posted cyber-bullying material targeted at an Australian child, has failed to comply with the Commissioner's notice, and the Commissioner is of the opinion that the police could appropriately have regard to the person's conduct under criminal law.

The cyber-bullying notice regime would apply to posted cyber-bullying material on social media services or any other relevant electronic service including email, text messages, instant messages, online games and chat functions on websites.

To reduce duplication and minimise the number of complaints handled by the Commissioner, the Commissioner will work with schools and police to establish processes to work together, undertake an information campaign to outline the purpose and role of the Commissioner and develop guidelines for handling reports of cyber-bullying (including reports of cyber-bullying arising through the proposed Australian Cybercrime Online Reporting Network (ACORN)).

The Commissioner will work with the police and schools to develop referral mechanisms to deal with cyber-bullying complaints more quickly and effectively.

Impacts on stakeholders

This option would not result in any new regulatory costs. However it is expected that this option would have a similar educative function to option (b) in raising awareness of the consequences of cyber-bullying.

What is the likely net benefit of each option?

The costs and benefits of each option will be assessed in a similar manner as to the assessment for options in Appendix D.

a. Status quo

Maintaining the status quo is the least resource intensive option.

However, this would mean that the current inefficient arrangements for dealing with cyber-bullying would remain and the negative impact of cyber-bullying would continue and perhaps grow. It should be noted that:

- cyber-bullying complaints that cannot be dealt with at the school level are generally directed to local police who have limited resources or skills to deal with these complaints, particularly those that do not warrant a criminal law response;
- there is limited awareness of the existing legal remedies; and
- pursuing criminal proceedings for cyber-bullying can lead to re-victimisation of the child.

The Government has made an election commitment to do more to protect children online.

	General instances	Exposure to material	Further behaviours
Harm*	5	5	5

Regulatory cost	Low (commensurate with other options) – no new regulation

*Harm - (1 = significant increase; 5 = no change; 10 = significant decrease/no more instances, exposure, or further behaviours).

b. Implement education and awareness raising measures to better explain the application of the current offence

Greater education and awareness-raising measures would be directed at children, those charged with the welfare of children and law enforcement.

Educational initiatives are non-regulatory and have the potential to improve policy outcomes through better awareness and enforcement of the laws already in place.

Some of the benefits of the existing Commonwealth Criminal Code offences are as follows:

- covers a range of conduct: the conduct may be explicit and contained in the content of the communications, or implicit and inferred by the type of use (e.g. multiple postings on a website), as long as a reasonable person would regard the conduct as being menacing, harassing or offensive;

- uses an objective standard: 'reasonable persons' must regard the use of the carriage service as menacing, harassing or offensive for an offence to be committed. This allows community standards and common sense to be taken into account when determining whether conduct is menacing, harassing or offensive;
- allows alternative sentencing options based on relevant state or territory sentencing options, such as a community service order; and
- since coming into effect in 2005, has been used to support 308 successful prosecutions for a broad range of conduct involving the internet, including eight prosecutions involving defendants under 18 years of age.

More may need to be done to raise awareness about the existing law and its application to cyber-bullying. This could increase the effectiveness of the existing law in deterring cyber-bullying.

Increasing education and awareness of the existing cyber-bullying offences was supported by a number of submissions to the public consultation, including by industry, child welfare and community organisations and legal bodies.

Greater education and awareness-raising measures would ensure young Australians more clearly understand that cyber-bullying can constitute an offence and that a broad range of sentencing options may apply. However, merely raising awareness about potential criminal consequences of cyber-bullying may have only limited impact. It is likely that the existing problems with police failing to deal with any but the most serious of cyber-bullying complaints will remain.

A key function of the Commissioner will be to promote online safety for Children, including through improved education and awareness raising activities.

	General instances	Exposure to material	Further behaviours
Harm*	7	5	7

Regulatory cost	Low (commensurate with other options) – no new regulation

*Harm - (1 = significant increase; 5 = no change; 10 = significant decrease/no more instances, exposure, or further behaviours).

c. Create a separate cyber-bullying criminal offence covering conduct where the victim is a minor, with a lesser maximum penalty

The creation of a new criminal offence would affect minors, those charged with the welfare of children, police and judicial staff.

This option may cause a potential increase in reporting of cyber-bullying to police, who have limited resources to respond to cyber-bullying matters. It may also increase the resourcing burden on the court system.

There are also social costs associated with this option, including:

- the possibility that it may over-extend to behaviour which should not be treated as a criminal offence and encourage over-reporting of incidents;
- more minors being charged with criminal offences, thereby increasing pressure on the legal system, and increasing trauma for offenders and victims due to the seriousness of criminal sanctions; and
- a new law may cause confusion regarding the application of the existing offence.

The benefits of creating a mid-range cyber-bullying offence include:

- a more effective deterrent to cyber-bullying behaviour;
- the new offence could use language that would be easier for minors to understand;
- an increased likelihood of prosecution for mid-range offending given a maximum penalty that is more proportionate to such offending by minors; and
- an opportunity to raise the awareness of students, parents and teachers about the legal consequences of cyber-bullying.

Although support for a new cyber-bullying criminal offence was evenly divided amongst submissions to the public consultation, the costs of implementing and enforcing a new offence outweigh the benefits it would provide. Further, it is probable that the existing problems with police failing to deal with any but the most serious of cyber-bullying complaints will remain.

	General instances	Exposure to material	Further behaviours
Harm*	6	5	9

Regulatory cost	Low (commensurate with other options) – new regulation mirrors existing law, but limits application to minors and has a commensurate lower penalty

*Harm - (1 = significant increase; 5 = no change; 10 = significant decrease/no more instances, exposure, or further behaviours).

d. Create a separate cyber-bullying notice regime to deal with cyber-bullying behaviour

A cyber-bullying notice regime would affect victims and perpetrators of cyber-bullying, and those charged with the welfare of children.

It would create an increased deterrent to cyber-bullying behaviour and reduce the pressure on police resources.

Benefits of this option include:

- civil and prevention based behavioural interventions are preferred to criminal sanctions, especially in relation to minors;
- would be a more expedient process for dealing with cyber-bullying;
- would address socially undesirable behaviours which cause cyber-bullying and would act as a deterrent to re-offending;
- an opportunity for the Commissioner to raise the awareness of perpetrators of cyber-bullying about the legal and other consequences of cyber-bullying.
- would reduce physical and mental harm caused by cyber-bullying; and
- may take some of the resourcing burden off schools and police in dealing with cyber-bullying issues.

The implementation of a civil regime was supported by a range of submissions to the public consultation, including child welfare and community organisations, the Australian Federal Police and the Law Council of Australia. Further, it would specifically target the identified gap between schools and law enforcement in handling complaints about cyber-bullying.

	General instances	Exposure to material	Further behaviours
Harm*	6	8	9

Regulatory cost	Low (commensurate with other options) – new regulation, but cost with complying are not considered as regulatory costs for purposes of the RIS.

*Harm - (1 = significant increase; 5 = no change; 10 = significant decrease/no more instances, exposure, or further behaviours).

Of the options identified above, option (d) is considered to have the highest net benefit on the basis that it would have a commensurate level of regulatory costs to the other three options, but would produce equal or greater benefits in terms of reducing harm from cyber-bullying material in comparison to the other options. Option (b) is also considered to be favourable on the basis that it would greatly reduce the harm caused from general instances of cyber-bullying, while having a very low regulatory impact.

This is summarised in the table below. The preferred options are highlighted.

Option	Harm from number of general instances*	Harm from exposure to material*	Harm from further behaviours*	Regulatory cost
Status quo	5	5	5	Low
Education and awareness raising measures	7	5	7	Low
New cyber-bullying offence	6	5	9	Low
New cyber-bullying notice regime	6	8	9	Low

*Harm - (1 = significant increase; 5 = no change; 10 = significant decrease/no more instances, exposure, or further behaviours).

Appendix F

Quality assurance of online safety programmes offered in schools

Research commissioned by the Department of Communications into youth awareness of cyber-bullying as a criminal offence provides supplementary evidence that schools are not providing best practice education on cyber-bullying, with the research identifying that:[87]

- only 63 per cent of youth agreed that cyber-bullying could be considered an offence punishable by law; and
- youth had a very low level of understanding that defamation (or 'saying something untrue about others') online could definitely be a crime (26 per cent).

In the absence of a certified approach to online safety education of parents, carers, teachers and children, Government cannot be certain that threats to Australian children, particularly in regard to cyber-bullying, are being adequately and authoritatively addressed.

In order for educational programmes about online safety to be effective, online safety messages must be thorough, consistent, factual, engaging and tailored to the needs of the audience.

Two policy options are discussed below, including:

a. status quo (non-regulatory); and

b. voluntary certification process.

a. Status quo (Non-regulatory)

All forms of abuse have a detrimental effect to a person's mental and physical health. Victims of cyberbullying can experience significant social isolation and feel unsafe. It can lead to emotional and physical harm, loss of self-esteem, feelings of shame and anxiety, concentration and learning difficulties. Incidents of young people committing suicide have also been linked with cyberbullying.

Schools are commissioning a range of third-party providers to deliver online safety programmes through face-to-face presentations, video conferencing and online/desktop software. This online safety education commonly covers issues such as cyber-bullying, keeping personal information private and how to stay safe online.

However, there is no standard of quality that these programmes and its provider must meet in order to be delivered in schools. Decision makers have no guidance in assessing the appropriateness and effectiveness of programmes about online safety offered in the market. As a result, programmes may deliver inaccurate information or ineffective advice and may not raise awareness of the potential for cyber-bullying to be considered a criminal offence under existing laws.

Maintaining the status quo, ad-hoc approach to online safety education will mean that Australian children, their parents and carers may receive programmes that are of inadequate quality to properly address the harmful effects of cyberbullying.

[87] website

b. Voluntary certification process

In the policy to *Enhance Online Safety for Children*, the Government committed to establishing a voluntary process for the certification of programmes about online safety that are offered in schools.

The voluntary process will certify providers (rather than individual programmes) to minimise the burden on industry. This will also allow providers more flexibility to update their programme content without having to reapply frequently for certification. Additionally, the $7.5 million grants funding programme will require that schools can only engage programmes about online safety from certified providers. By linking the two initiatives, schools that receive funding under the grants programme will be able to make more informed decisions regarding the online safety education delivered in their school community.

The voluntary certification process will focus on the ability of providers to deliver appropriate and effective online safety programmes with some limited criteria regarding programme content. This light touch approach will help schools identify the providers that are already providing high quality programmes to schools, as a by-product, some providers may update their programmes so they can be considered for certification.

Consultation will be undertaken with education authorities and industry to ensure that the certification guidelines meet the needs of education authorities and schools, without introducing unnecessary burden on programme providers.

The Commissioner will also undertake information campaigns targeted at education authorities and schools to communicate the benefits of purchasing programmes from certified providers. The specifics of the voluntary certification programme will be a matter for the Commissioner.

Impacts on stakeholders

The application of Voluntary Certification and assistance with the provision of online safety education programmes in Australian schools will assist in securing efficiencies in the choice of programmes to schools and teachers. It should have the consequential effect of reducing the incidence of cyber-bullying in schools. There will be minor additional costs for education providers participating in the certification process.

What is the likely net benefit of each option?

The costs and benefits of each option will be assessed in a similar manner as to the assessment for options in Appendices D and E.

a. Status quo

Maintaining the status quo is the least resource intensive option. However, the wide range of providers and their programmes about online safety can make it difficult for schools to determine which providers offer effective programmes to help their school community respond to cyber-bullying.

The Government has made an election commitment to do more to protect children online and to increase the support provided to teachers so they are better equipped to manage the online activity of children in their care.

	General instances	Exposure to material	Further behaviours
Harm*	5	5	5

Regulatory cost	Low (compared to other options) – no new regulation

*Harm - (1 = significant increase; 5 = no change; 10 = significant decrease/no more instances, exposure, or further behaviours).

b. Voluntary certification process

This option would affect programme providers from a range of different sectors including, industry, community organisations and government.

Participation in the process would be optional for industry and those providers who choose to participate would not be subject to onerous administrative requirements. Applicants would incur costs in applying for certification and complying with any limited reporting requirements under the process.

The Department has consulted with stakeholders on the assumptions underpinning the regulatory costing of this option. Further detail on the feedback received is outlined at Appendix G. In estimating the regulatory impact on industry of participating in a voluntary certification process, the Department has assumed that 10 online safety programme providers currently providing programmes in primary schools will apply for certification. Each provider will allocate 35.5hrs in the first year (9.0hrs in each successive year) to the following activities:

- Familiarisation with certification guidelines
- Preparation of certification application documents and completion of an application form
- Completion of a certification agreement with the Commissioner
- Cost of undertaking or updating police and working with children checks
- Changes to current training product including: adding certification branding to programme website and promotional material; communicating changes to current users; and updating any software product
- Establishing a contact person for the Commissioner to engage with, and
- Providing an annual statement to the Commissioner concerning compliance with the certification agreement.

This option would deliver increased social benefits by allowing schools that choose programmes from providers that have been evaluated as effective for increasing participants' capacity for preventing, managing and reporting cyber-bullying and other harmful content.

	General instances	Exposure to material	Further behaviours
Harm*	7	7	7

Regulatory cost	Low/medium (compared to other option) – there would be costs involved with organisations applying for voluntary certification from the Commissioner and complying with any limited reporting requirements under the process. However participation in the process would be optional for industry and those providers who choose to participate.

*Harm - (1 = significant increase; 5 = no change; 10 = significant decrease/no more instances, exposure, or further behaviours).

Of the options identified above, option (b) is considered to have the highest net benefit on the basis that, while it would involve slightly higher costs for participants, such costs would be voluntary, and the certification of providers of programmes would lead to a higher reduction in harm from cyber-bullying material in comparison to option (a).

This is summarised in the table below. The preferred option is highlighted.

Option	Harm from number of general instances*	Harm from exposure to material*	Harm from further behaviours*	Regulatory cost
Status quo	5	5	5	Low
Voluntary certification	7	7	7	Low/medium

*Harm - (1 = significant increase; 5 = no change; 10 = significant decrease/no more instances, exposure, or further behaviours).

Appendix G

Stakeholder Feedback

This appendix summarises stakeholder's views on the draft Regulatory Impact Statement. For the purposes of confidentiality, commentary and responses referred to below have been de-identified.

What views were expressed by stakeholders?

Stakeholders provided a range of comments in relation to the draft RIS. Stakeholders were generally supportive of the policy proposal outlined, acknowledging the considerable work which has been undertaken by the Government in advancing the election commitment to establish a Children's e-Safety Commissioner and implement a legislatively backed complaints system.

Stakeholders also noted that they were pleased to see that many of their recommendations from the public consultation phase had been incorporated into the draft legislation.

Some concerns were noted by government stakeholders that there is a lack of research around how or why children engage in suicidal behaviour and self-harm and accordingly the establishment of the Commissioner should not be presented as the main means to either combat bullying or address intentional self-harm or suicidal behaviours among children. In this regard, note that the preferred option combines a number of measures which will work in parallel with existing initiatives currently utilised by the States and Territories, non-profit organisations and social media services.

Child welfare groups noted that there should be a greater focus on parental education. These stakeholders suggest that more funding should be invested into areas of support and education for parents. These comments will be taken into account as work on the Voluntary Certification Process progresses.

Were assumptions validated by stakeholders?

The Department consulted with stakeholders on the assumptions underpinning the regulatory costing for measures to enhance online safety for children.

In relation to the quality assurance of online safety programmes offered in schools, existing programme providers generally supported the proposed policy and did not object to the assumptions. One provider commented that the Voluntary Certification Process (VCP) could duplicate the requirements for the Harm Prevention Charity Status resulting in additional workload and cost for applicants. The Department will have regard to this comment as work on the Voluntary Certification Process progresses, however on an initial view the Harm Prevention Charities Register is heavily focused on charities and their access to taxation benefits and may have limited use for the certification process. An existing program provider also commented that in finalising any guidelines for certification, consideration should be given to exceptions to reporting requirements and updating of programs for registered not-for-profit charities. This also will be considered as the guidelines are developed.

Significant feedback was received on the assumptions underpinning the costings for the rapid removal scheme. Social media service stakeholders provided valuable input on the time and resource requirements likely to be involved for social media services under tier 1 of the preferred, two-tier scheme. However two claims by providers were not supported.

The first of these is the premise that a rapid removal scheme may result in an increase in the volume of reports being made to social media services. Social media sites have advised that they invest heavily in reporting tools and encourage their users to report any abuse, including bullying and harassment, directly to them. Given the extent of investment in these tools and the promotion of these by sites, it is not clear that the establishment of the Commissioner would result in any complaints being made that are not already being raised with the sites. Further, social media sites have not provided any evidence to back their claim that complaint volumes will increase. As a result, it is not expected that there would be any costs flowing from a rise in complaints, and if there was a rise, it would be expected to be relatively modest.

The second premise is that the ongoing maintenance and upkeep of complaints handling systems in order to retain standing within tier 1 and avoid falling into tier 2 should be considered as compliance costs. This is not supported. Business as usual costs are not considered as regulatory costs.

An industry stakeholder warned of the possible risk of unintended regulatory costs caused should key definitions or requirements in the legislation lead to 'over capture', or in other words, if the legislation establishing the rapid removal scheme was worded too broadly and in a way that affected stakeholders other than social media providers. Key stakeholders have been consulted closely in developing the legislation to give effect to the rapid removal scheme to minimise this risk.

A range of stakeholders raised the issue of possible regulatory costs should new data access or information gathering regimes be required. No new regimes are being proposed; it is envisaged that the Commissioner will be able to rely on similar powers to those available to the ACMA.

An industry stakeholder noted that the 'net benefit assessment involves consideration of the regulatory cost of relevant policy decisions.' This stakeholder advised that the RIS provides a rationale for the policy focus on this issue and provides an accurate account of the measures taken by the Government to comply with best practice policy development processes.

Did stakeholders suggest any alternative policy approaches?

A number of stakeholders suggested alternative policy approaches.

Some stakeholders advised that an alternative option to the rapid removal scheme is to provide additional resources to the Complaints Handling Protocol. This option has been considered as part of the option to continue the status quo in Appendix D. This option is not preferred, and is inconsistent with the Government's election commitment.

Government stakeholders also discussed the need for the RIS to reflect that a wide spectrum of cyber-bullying behaviours exist which are not necessarily criminal in nature and that only behaviour that is sufficiently serious is able to be dealt with by police. Comments were also received around support for a framework which minimises duplication of complaints handled by the Commissioner, including those arising through the Australian Cybercrime Online Reporting Network.

As noted above, some online safety programme providers noted that another option includes a greater focus on parental education.

Is the preferred option generally supported?

Overall, the preferred option was generally supported by stakeholders and this was reflected in the submissions received in response to the consultation process. There were a small number of suggested amendments including commentary from an industry stakeholder who submitted that the RIS provides a rationale for the policy focus on the issue of cyber-bullying, and an accurate account of the measures taken by the Government to comply with best practice policy development processes. That stakeholder recommended that the legislation be clearly and unambiguously expressed in order to minimise the "risk of 'over capture' and 'unintended consequences on industry and individuals'.

It should be noted that social media services have publicly expressed the view that there is no need for new regulation in relation to cyber-bullying material on their services as they already have in place significant resources and systems in place to deal with this type of material. This is acknowledged, and recognised in the Government's preferred option to introduce a two-tier system where regulatory compliance will only be mandatory for large social media services which do not have well-established and robust complaints handling procedures and systems.

Overall, stakeholders support the Government's initiatives to enhance online safety for children, and in the context of the RIS, would agree that those initiatives could be expected to have a net benefit.

Appendix H

Regulatory burden and cost offset estimate

Average Annual Regulatory Costs (from Business as usual)				
Change in costs ($million)	**Business**	**Community Organisations**	**Individuals**	**Total change in cost**
Total by Sector	$0.432	$0	$0	$0.432
Cost offset ($million)	**Business**	**Community Organisations**	**Individuals**	**Total by Source**
Agency	($21.77)	$0	$0	$(21.77)
Are all new costs offset? ☑ yes, costs are offset ☐ no, costs are not offset ☐ deregulatory, no offsets required				
Total (Change in costs - Cost offset) ($million) ($21.34)				

The regulatory cost offsets noted in the above table have been identified within the Communications portfolio. These cost offsets relate to the Identity Checks for Prepaid Mobile Services reforms.