Australian Government

Department of Communications

Enhancing Online Safety for Children

Public consultation on key election commitments

January 2014

GPO Box 2154 Canberra ACT 2601 Australia • telephone 02 6271 1000 • website http://www.communications.gov.au

Contents

Public Consultation Process

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

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

The Department of Communications (the Department) is seeking views on the issues raised in this discussion paper to assist in providing advice to the Government to enhance online safety for children. This paper is for consultation purposes only and does not necessarily represent current government policy.

Questions are included in boxes throughout the paper to guide discussion. Respondents are invited to provide written submissions or comments to address these questions, or provide a more general response if preferred.

Submissions must include the respondent's name, organisation (if relevant) and contact details. Submissions with no verifiable contact details will not be considered.

Respondents should be aware that submissions will generally be made publicly available, including on the Department's website (www.communications.gov.au). The Department reserves the right not to publish any submission, or part of a submission, which in the view of the Department contains potentially defamatory material, or where it considers it appropriate to do so for confidentiality or other reasons.

All submissions will be treated as non-confidential information unless the respondent specifically requests the submission, or a part of the submission, is kept confidential, and acceptable reasons accompany the request. Email disclaimers will not be considered sufficient confidentiality requests. Note that submissions will generally be subject to the *Freedom of Information Act 1982*.

The *Privacy Act 1988* establishes certain principles with respect to the collection, use, and disclosure of information about individuals by the Department. Any personal information respondents provide to the Department through their submission is used only for the purposes of consideration of issues raised in this paper. Respondents should clearly indicate in their submission if they do not wish to have their name included in any summary of submissions that the Department may publish.

The closing date for submissions is **5.00 pm, 7 March 2014**.

Submissions can be lodged in the following ways:

Email: onlinesafety@communications.gov.au

Post: The Director, Cyber Safety Policy and Programs
Department of Communications
GPO Box 2154
CANBERRA ACT 2601

Introduction

The dominance of internet use and social media

The internet has become a daily, integrated part of life for many Australian families. It is an essential tool for all Australians, an integral part of our economic and social activities, and a vast resource of information, education and entertainment. The ability for young Australians to use online tools effectively provides both a skill for life and the means to acquire new skills. The internet provides children with a means through which they can exchange information, be entertained, socialise, do school work and conduct research.

Studies show that over 95 per cent of young Australians use the internet regularly.[1] Almost daily internet use is common for children as young as eight or nine. This rapidly changes in the 'tween' years with many 10-12 year olds using the internet from 1-3 hours per day. By 13, social media use has become the norm; and by 15, the internet and its use has become an 'organic integrated part' of the everyday lives of Australian children.[2] Whilst the popularity of various online activities – including email, games, chat, shopping, and passive consumption of music and videos – varies with different age groups, social media use has 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 digital means such as text messages, phone calls and email.[3] While around half of young Australians aged between 8 and 11 years use social media sites, this figure dramatically increases to around 90 per cent for 12 to 17 years olds.[4] Research on the specific social media usage habits of children and young people indicates that the small minority of 12-17 year olds that do not have a Facebook account (usually due to parental control) felt that they suffer a degree of social isolation and exclusion.[5]

This increased exposure to the internet and social media is also enhanced with the increase 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;[6] and
- around half of 14-17 year olds access the internet through mobile phones,[7] with 43 per cent of them having their own smartphone.[8]

---

[1] Young and Well Cooperative Research Centre, *Using technology safely and effectively to promote young people's wellbeing*, March 2013, pg. 2
[2] Australian Communications and Media Authority, *Like, post, share: Young Australians' experience of social media - Qualitative research report*, August 2011, pg. 15
[3] Australian Communications and Media Authority, *Like, post, share: Young Australians' experience of social media - Qualitative research report*, August 2011, pg. 26
[4] Australian Communications and Media Authority, *Click and connect: Young Australians' use of online social media – 02: Quantitative research report*, Commonwealth of Australia, 2009, pg. 8
[5] Australian Communications and Media Authority, *Like, post, share: Young Australians' experience of social media - Qualitative research report*, August 2011, pg. 23
[6] Telstra, *Safer internet and back to school survey* (internal report), January 2013

The growing number of Australian children accessing the internet and social media through mobile devices is significant and highlights the capacity for children's internet activities to, in some instances, occur 'under the radar' of parents, teachers and other supervising adults. In this new digital environment, with more children independently using the internet and social media, the Government is seeking to address the online safety risks, such as cyber-bullying, that are also increasingly affecting Australian children.

A recent study into cyber-bullying in Australia published in the *International Journal of Children's Rights* defines cyber-bullying as 'any communication, with the intent to coerce, intimidate, harass or cause substantial emotional distress to a person, using electronic means to support severe, repeated and hostile behaviour'.[9] Cyber-bullying can occur in a variety of ways, through a range of digital devices and mediums, most commonly smartphones and social media sites.[10] On social media sites cyber-bullying can be content-driven, such as posting embarrassing or harmful photos, videos, or rumours relating to an individual. These are often exacerbated by other social media features (such as 'comments', 'shares' and 'likes') which serve to actively promote and spread the harmful content at a rapid rate, and to a wide audience.

The Australian Communications and Media Authority's (the ACMA) research indicates four per cent of eight to nine year olds; 21 per cent of 14-15 year olds; and 16 per cent of 16-17 year olds reported being cyber-bullied.[11] 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.[12]

Some of the more extreme cases of cyber-bullying have resulted in young children committing 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 the range of risk factors associated with youth suicide, with victims of cyber-bullying possessing vulnerability characteristics known to be present in suicide deaths. The study showed that youth suicide statistics linked to bullying in Queensland alone were grim, and various advocacy organisations, including the Australian Human Rights Commission, have called for more serious treatment of cyber-bullying as an issue harming the welfare of Australian children.[13] Media articles have reported the following instances:

---

[7] Australian Communications and Media Authority, *Like, post, share: Young Australians' experience of social media - Quantitative research report*, 2013, pg. 22

[8] Australian Communications and Media Authority, *Communications report 2011-12*, Commonwealth of Australia, Melbourne, 2012, pg. 35

[9] Definition of cyber-bullying contained in *Megan Meier Cyberbullying Prevention Act* Sec 88_1(a), cited in Srivastava, Gamble & Boey, *Cyberbullying in Australia: Clarifying the Problem, Considering the Solutions*, International Journal of Children's Rights 21 (2013) 25-45, May 2013, pg. 27

[10] Srivastava, Gamble & Boey, *Cyberbullying in Australia: Clarifying the Problem, Considering the Solutions*, International Journal of Children's Rights 21 (2013) 25-45, May 2013, pg. 29

[11] Australian Communications and Media Authority, *Like, post, share: Young Australians' experience of social media - Quantitative research report*, 2013, pg. 10

[12] McAfee's *Tweens, Teens and Technology* report, May 2013

[13] For examples see *The Queensland Commission for Children and Young People and Child Guardian*, 28 June 2013 and media articles: The Courier Mail, *13 child suicides in three years prompt call for action as bullying victims take their own lives*, 24 May 2013; The Australian, *Family of suicide teen Sheniz Erkan urge parents to*

- in September 2013, a Tasmanian 15-year-old schoolgirl took her own life after being bullied, including cyber-bullied;[14]
- a 13-year-old Sydney girl took her own life in April 2013 after bullies relentlessly pursued her;[15]
- a 14-year-old Melbourne schoolgirl took her own life in January 2012 after suffering bullying unknown to her parents;[16] and
- in 2009, a Melbourne mother blamed her 14-year-old daughter's suicide on the internet and the tragic case has highlighted the problem of cyber bullying among young people.[17]

Prior to the federal election in September 2013, the Coalition released its *Policy to Enhance Online Safety for Children*, with a view to specifically address these risks in relation to children, so that content and cyber-bullying concerns are handled faster; children can quickly access assistance with online safety concerns; Commonwealth criminal laws relating to cyber-bullying are appropriate and effective; and there is clear and expert leadership in online safety.

The policy sets out the commitment to:

- establish a Children's e-Safety Commissioner to take the lead across government in implementing policies to improve the safety of children online;
- develop an effective complaints system, backed by legislation, to get harmful material down fast from large social media sites; and
- examine existing Commonwealth legislation to determine whether to create a new, simplified cyber-bullying offence.

This discussion paper outlines aspects of these commitments for consideration. The Department invites comments on the policies outlined in this paper, as well as discussion of the specific questions posed in each chapter.

Regulatory measures in this area must of course take account of the underlying importance of freedom of expression to the Australian community. If measures proposed have the potential to impact on freedom of expression, then it is important that they are reasonable and proportionate to the intended policy goal of improving the online safety of Australian children.

---

watch children's internet use 13 January 2012; and The ABC, *Teens death highlights cyber bullying trend*, 23 July 2009

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

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

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

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

1. Establishment of a Children's e-Safety Commissioner

As part of the election campaign in September 2013, the Government committed to appoint a senior Commonwealth official as a Children's e-Safety Commissioner (the Commissioner), supported by existing resources re-allocated from existing locations within the public service. The Commissioner will be a single point of contact for online safety issues for industry, Australian children and those charged with their welfare. The Commissioner will also take the lead across government in implementing policies to improve the safety of children online.

The need for an accessible and centralised point of contact to deal with online safety has been recognised by policy makers in a range of contexts. For example, on 5 November 2013 the New Zealand Government introduced the *Harmful Digital Communications Bill*, which proposed the appointment of an Approved Agency under a new civil enforcement regime to handle complaints about harmful digital communications and assist in dispute resolution.[18] The Victorian Law Reform Committee also recommended the establishment of a Digital Communications Tribunal.[19]

1.1. Functions of the Commissioner

The Government's election policy commitments indicate that the Commissioner will have responsibility for the following:

- implementing the proposed scheme for the rapid removal of material that is harmful to a child from large social media sites (outlined in Chapter 2);
- working with industry to ensure that better options for smartphones and other devices and internet access services are available for parents to protect children from harmful content;
- establishing an advice platform with guidelines for parents about the appropriateness of media content;
- establishing a research fund to consider the effects of internet use on children, how support services can be provided online and how to mitigate children's online risks;
- establishing a voluntary process for the certification of online safety programmes offered within schools; and
- establishing a funding programme for schools to deliver online safety education.

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

---

[18] *Harmful Digital Communications Bill*, New Zealand Parliament, 5 November 2013. The first reading of the bill was on 3 December 2013 and it was referred to the Justice and Electoral Select Committee for consideration. Submissions are due with the Justice and Electoral Select Committee by 21 February 2014, and the Committee's report is due by 3 June 2014.

[19] Victorian Law Reform Committee, *Report of the Law Reform Committee for the Inquiry into Sexting*, May 2013, pg. 201

Refer to Appendix A for a list of existing Australian Government online safety programmes and resources.

The clear policy intent of the Government is to have a single organisation which takes the lead in relation to online safety for children, allowing for greater efficiency and addressing duplication and overlap. There may, however, be some offsetting considerations in weighing up which programmes should be transferred to the Commissioner's control. For instance, while some resources and research projects specifically target online safety for children (such as the Cybersafety Help Button and Australian Children's Cybersafety and E-security Project), other resources are intended for improving the online safety of people of all ages and therefore may not be suited to a Children's e-Safety Commissioner. For example, the Australian Federal Police's (AFP) *ThinkUKnow* programme involves the delivery of public safety messages to students, teachers and parents, which are bolstered by the law enforcement role that the AFP has within the community. The 'Report Abuse' function of the *ThinkUKnow* programme is used to report online grooming behaviour. Consideration should be given to whether the 'Report Abuse' function should also remain with a law enforcement body.

In cases where any agencies retain their online safety programmes, the Commissioner would be expected to establish strong working relationships to ensure consistent messaging in online safety initiatives, and to avoid duplication with the delivery of other online safety programmes.

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

1.2. Establishment of the Commissioner

A range of options are available for establishing the Commissioner. Best practice principles for establishing a new government position are outlined in the *Governance Arrangements for Australian Government Bodies*[20] published by the Department of Finance, which include some of the following key principles:

- There should be no unnecessary proliferation of government bodies, therefore a new function, activity or power should be conferred on an existing body, unless there is a persuasive case to form a new body.
- Existing governance structures allow for well-understood lines of responsibility to operate, including the clear application of other accountability laws and processes.
- A departmental status works well for functions of government that require close ministerial involvement, direction and responsibility.
- Additional set-up and ongoing administrative costs for the body should be minimised to reduce demands placed on public sector resources.

[20] *Governance Arrangements for Australian Government Bodies*, Australian Government Department of Finance, August 2005

- A balance needs to be struck between establishing a body's independence while at the same time still enabling government to govern efficiently.

It is a key objective that the Commissioner will maintain a high public profile to provide visible leadership on enhancing online safety for children.

Option 1 – establishment of an independent statutory authority

This option would see the creation of a new independent statutory authority, separately staffed and resourced to support the Commissioner and its functions. While this option would provide the greatest level of independence for the Commissioner to carry out his/her functions, it is also the most costly option.

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

This option would establish a Commissioner as an independent office, and provide that office with administrative support from an existing government agency (an approach recently taken by the Australian Energy Regulator, which was established as an independent Statutory Board with administrative resources sourced from the Australian Competition and Consumer Commission).

Administrative support could be provided by the ACMA, with relevant existing ACMA powers delegated and resources transferred to the Commissioner. Alternatively, administrative support could be provided by the Department of Communications. This would provide some synergies in policy development activities between the Commissioner and the Department, but may give the impression that the Commissioner is not sufficiently independent from government.

Option 3 – designation of a Member of the ACMA as the Commissioner

This option would involve appointing an existing member of the ACMA Board to be the Commissioner, with legislative amendments to the *Australian Communications and Media Authority Act 2005* (the ACMA Act) to permanently place the role of the Commissioner within the ACMA Board, with distinct functions and powers to achieve the Commissioner's intended purpose.

One benefit of this approach is that it would be possible to temporarily appoint an ACMA Member to act as the Commissioner while legislative arrangements are established for the permanent Commissioner and his/her functions (including legislation for the proposed scheme for rapid removal of material that is harmful to a child from social media sites – see Chapter 2). Having interim arrangements would enable a more rapid transition to the new arrangements, as the interim Commissioner could be closely involved in setting up the legislative arrangements for the new Commissioner.

A variant of this option would see the appointment of an Associate Member of the ACMA as the Commissioner, with distinct functions and powers to achieve the Commissioner's intended purpose. An advantage of this variant is that the appointment could be made without legislative amendment to the ACMA Act.

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

This option would involve establishing a legislated framework for appointing an expert non-government organisation (NGO) to undertake the role of the Commissioner. The NGO would be selected on a competitive basis and would operate under contractual arrangements with

government. The contract would set out the quantity and quality of outputs the selected NGO would deliver.

This option is similar to an approach being proposed in New Zealand under the new *Harmful Digital Communications Bill*.[21]

The key advantage of this option would be the greater flexibility that NGOs have in terms of their:

- operating cost structure;
- capacity to work with industry, including generating additional income; and
- capacity to work with state and territory agencies, including law enforcement and education agencies.

A potential disadvantage may be limits on the range of 'enforcement' functions that an NGO is allowed to take on. This may require the selected NGO to work closely with local police.

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

[21] *Harmful Digital Communications Bill*, New Zealand Parliament, 5 November 2013

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

While social media offers many benefits, the increase in use of social media in the general community has created an enormous amount of content relating to individuals online. Content uploaded to popular social media sites has the potential to be viewed by large audiences and go viral quickly. User generated content is not always created with forethought or discretion, and the increasing instances of cyber-bullying, sexting and 'revenge porn' are particularly concerning when young people are involved.

The Government consulted widely, while in Opposition, with parents, teachers, children and many others with interest and expertise in the issue of online safety for children. It was clear from that consultation process that today there are inadequate remedies available when children are the victims of harmful, aggressive and bullying material targeted at them using the internet. There have been multiple, tragic instances of suicides in response to cyber-bullying.

One of the outcomes of the National Bullying, Young People and the Law Symposium, which was held in July 2013, was the recommendation:

> The Federal Government to establish a national digital communication tribunal with the power to act, speedily and in an informal manner, to direct the immediate removal of offensive material from the internet.[22]

In addition, 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. Social networks, governments, educators, parents/carers and youth advocates all have a role to play in ensuring that quick and effective help is available for young people who need it. The Government's policy clearly recognises that it's time for key stakeholders to do more to assist young people facing online dilemmas, and that in the online world, rapid removal is synonymous with protection.

Consultations with the Youth Advisory Group on Cyber Safety (YAG) and the Teachers and Parents Advisory Group on Cyber Safety (TAP) have also highlighted the need for harmful online content to be dealt with more effectively and quickly. The YAG and TAP consultations in 2013 indicated that YAG and TAP members recommend social media sites should respond more promptly to reported issues and should provide confirmation that action has been taken.

[22] Recommendations of the *Bullying, Young People and the Law Symposium*, Australia, 18-19 July 2013

The following measures are currently available to Australians for dealing with online safety concerns. The existing complaints-handling mechanisms (outlined below) combine regulatory and non-regulatory measures.

Existing arrangements for removal of online content

Cooperative Arrangement for Complaints Handling on Social Networking Sites[23]

Since early 2013, the *Cooperative Arrangement for Complaints Handling on Social Networking Sites* (the Protocol) has been in place. The Protocol 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. Compliance with the Protocol by industry is voluntary, and current signatories include Facebook, Google (YouTube), Yahoo!7 and Microsoft. The arrangements are not legally binding and there are no sanctions or consequences for failure to comply with the Protocol.

Online Content Scheme

Regulatory measures to deal with prohibited online content are provided in the Online Content Scheme set out in the *Broadcasting Services Act 1992*. The Online Content Scheme regulates illegal and offensive online content in Australia with reference to the National Classification Scheme.

Online content includes internet webpages, social media sites, live audio-visual streaming and links to content. It applies to content accessed on desktop computers, mobile phones and other convergent devices.

Prohibited content is content that has been classified by the Classification Board as Refused Classification (RC), X 18+, and R 18+ and MA 15+ content in certain circumstances.

Potential prohibited content is content that is assessed as likely to fall within a prohibited classification category if it were to be classified by the Classification Board.

Content is assessed on the basis of a complaint by a member of the public to the Hotline for reporting offensive and illegal online content administered by the ACMA where the complainant considers that the content may be prohibited under Australian law. The prohibitions are backed by strong sanctions for non-compliance, including criminal penalties for serious offences. The ACMA must investigate all valid complaints and referrals from other government agencies, and may also initiate its own investigations into online content.

If the ACMA finds content hosted in or, in relevant cases, accessed from Australia to be prohibited or potential prohibited content, it will direct the content provider to remove or prevent access to the content from their service, for example, issue a take-down notice.

[23] The Department of Communications uses the terms 'social media sites' and 'social networking sites' interchangeably. However, the Department invites comments at Question 3 of this discussion paper as to how these terms should be defined.

For prohibited content hosted overseas, the URL to the material must be added to the list of prohibited and potential prohibited URLs managed by the ACMA. This list is then provided to PC filter vendors accredited by the Internet Industry Association under the Industry Code of Practice. The ACMA regularly reviews URLs and provides revised lists to accredited vendors.

Regardless of where the content is hosted, if the ACMA considers the content to be of a sufficiently serious nature, such as child sexual abuse material, it must notify the police or another body as endorsed by the police. The Online Content Scheme also dovetails with the international system for rapid law enforcement notification and take-down that operates under the auspices of INHOPE – the International Association of Internet Hotlines.

The disadvantage of using the Online Content Scheme to address content complaints is that if the material is hosted in another country (as is the case in the great majority of instances), the ACMA does not have a legal mechanism to order the content host to remove the material.

Anti-discrimination legislation

In some situations, issues relating to online content can be the basis for complaints to the Australian Human Rights Commission (AHRC) under federal anti-discrimination law (for example, online content that is alleged to constitute sexual harassment or racial hatred). Where such complaints are made to the AHRC, the President is required to inquire into and attempt to resolve the complaint by conciliation. Where conciliation is not appropriate or unsuccessful the complainant may apply to the Federal Court of Australia or the Federal Circuit Court of Australia to have the allegations heard and determined. The AHRC has a dispute resolution rather than determination or enforcement role in relation to such complaints. Similar complaints options are also provided for under state and territory anti-discrimination law.

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.'[24]

While noting that some of the larger, more widely used social media sites have significantly improved their complaints handling processes in recent years, the fact remains that Australians currently have no recourse in instances where they may disagree with how their content complaints are handled by social media sites.

On this basis, the Government proposes to introduce a scheme to enable the rapid removal from a large social media site of material targeted at and likely to cause harm to a specific child (the proposed scheme). The proposed scheme will provide an independent and impartial third party to consider such disagreements between social media sites and individuals on content complaints, where the content relates to a specific child in Australia. By establishing the proposed scheme in

[24] Srivastava, Gamble & Boey, *Cyberbullying in Australia: Clarifying the Problem, Considering the Solutions*, International Journal of Children's Rights 21 (2013) 25-45, May 2013, pg. 37

legislation, it will help to build the confidence and trust of Australian families in how social media sites deal with their concerns.

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

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

2.1. Details of the proposed scheme

Participating social media sites

Using Boyd and Ellison's[25] definition, social networking sites[26] are web-based services that allow individuals to:

- construct a public or semi-public profile within a bounded system;
- articulate a list of other users with whom they share connections; and
- view and traverse their list of connections and those made by others within the system.

The Office of the Australian Information Commissioner defines social networking sites as 'websites that let people socialise online, send messages to one another, share interests, chat, meet people, and post information, photos and videos about themselves for others to look at.'[27]

Q3	Are these definitions of 'social networking sites' suitable for defining 'social media sites' for the purposes of this scheme?
Q4	Should the proposed scheme apply to online games with chat functions?

The Government has made it clear in its policy statement that it intends that the scheme will apply to large social media sites. The Government proposes the following approach in determining the range of social media sites which are included:

- The legislation will define a **large social media site** by reference to objective criteria such as the number of user accounts held with the site by Australians.

[25] Boyd and Ellison, *Social Network Sites: Definition, History and Scholarship*, Journal of Computer-Mediated Communication, 2008, Blackwell Publishing Limited

[26] The Department of Communications uses the terms 'social media sites' and 'social networking sites' interchangeably. However, the Department invites comments at Question 3 of this discussion paper as to how these terms should be defined.

[27] Website of the Office of the Australian Information Commissioner

- The legislation will define a **participating large social media site** as a **large social media site** which the Minister determines is a **participating large social media site** – it is likely the Minister would make such a determination having regard to whether the site has staff or assets in Australia or generates advertising revenue in Australia.
- If a site is not a **large social media site**, but its operator has volunteered in writing to the Minister to participate in the proposed scheme (presumably because it recognises the reputational benefits of doing so), this will be a **participating non-large social media site**.
- The proposed scheme will apply to **participating social media sites,** defined as being **participating large social media sites** and **participating non-large social media sites**.

Q5 What is the best criterion for defining a 'large social media site', and what available sources of data or information might be readily available to make this assessment?

Q6 Is the coverage of social media sites proposed by the Government appropriate and workable?

The Commissioner would publish a list of the participating social media sites. This would assist the public to know whether potential complaints are eligible to be handled under the proposed scheme.

Social media sites complaints system

The Government envisages that the legislation would require a company which operates a 'participating social media site' to put in place an acceptable complaints handling and rapid removal arrangement. The Commissioner would determine the criteria for such an arrangement and would be authorised to assess acceptability upon receiving a complaint about the site's processes or on the Commissioner's own initiative, for example, based on the volume of complaints. For this purpose, the company which is to be subject to the scheme is the company which has the ability to remove material from the site. It could be an Australian or foreign company.

Where the Commissioner finds that the complaints handling scheme of a participating site does not meet an acceptable standard, the Commissioner can issue an improvement notice. If the site fails to respond adequately to the improvement notice, the Commissioner would be empowered to make a public statement on the shortcomings of the sites' complaints handling processes. This public statement would be directed to parents, teachers and children.

Eligible complainant

The proposed scheme would define a category of people who are eligible to lodge a complaint about harmful material that is directed at a specific child. An **eligible complainant** would be:

- any person under the age of 18 (the child) who is the specific target of the harmful material; or
- the child's parent or guardian; or
- another adult in a position of authority in relation to the child (for example, a teacher or carer).

The child would have to be ordinarily resident in Australia.

If the complaint has been lodged by a parent, guardian or another person in authority, the consent of the child that is the target of the harmful material would need to be obtained.

Q7 Should the scheme allow children who are unsupported by adults to be active participants (either as complainants or notice recipients)? Having regard to the vulnerability of children, what procedural safeguards should be in place?

Form of complaints

The proposed scheme would require eligible complainants to report and request removal of the harmful material, in the first instance, to the participating social media site via the social media site's own established complaints system, before lodging a complaint with the Commissioner.

Complaints would be lodged with the Commissioner using a standardised online form, requiring certain basic information (including name and contact details of the complainant, clear identification of the material, identification of the participating social media site, and the outcome of attempted reports and requests lodged to the social media site to have the material removed). The Commissioner would be responsible for determining the content of the form.

Q8 What type of information would it be necessary to collect from complainants in order to assess their eligibility under the proposed scheme (including age verification), and also to adequately process complaints with minimal investigation required?

The Commissioner would not assess the complaint unless:

- the material remains available; and
  - the participating social media site has failed to adequately respond to the report within a specified timeframe; or
  - the participating social media site has responded to the report within the specified timeframe, however, has decided not to remove the material in question; or
  - the participating social media site does not provide an adequate mechanism for its users to report and request removal of material.

Q9 How would an eligible complainant demonstrate that the complainant has reported the content to the participating social media site?

Q10 What should the timeframe be for social media sites to respond to reports from complainants? Is 48 hours a reasonable timeframe, or is it too short or too long?

The Commissioner would not be required to investigate complaints that the Commissioner considered to be frivolous, vexatious or not made in good faith.

Q11 What level of discretion should the Children's e-Safety Commissioner have in how he/she deals with complaints?

Process for complaints handling – Stage 1

Upon receiving complaints that meet the objective minimum requirements, the Commissioner would automatically refer the complaint to the relevant participating social media site:

- advising of the complaint that has been received;
- seeking advice as to the status of the material in question; and
- advising that if the material remains available on the site, that the complaint will be assessed by the Commissioner, who may issue the social media site with a notice to remove the material.

The Commissioner would allow the relevant social media site a certain timeframe to respond to the initial referral.

Q12 What is an appropriate timeframe for a response from the social media site to the initial referral of the complaint?

The Commissioner would also automatically respond to the complainant to acknowledge receipt of the complaint.

Process for complaints handling – Stage 2

Following the response from the social media site in Stage 1, if necessary, the Commissioner would then assess the complaint and the material. Material which is the subject of a complaint would need to meet a statutory test in order for Stage 2 to apply (the Government proposes that the test should be '**material targeted at and likely to cause harm to an Australian child'**). The statutory test for such material would require:

- that the material which is the subject of the complaint would have to relate directly to the child in question;
- a reasonable person would consider that the material would be likely to cause harm or distress to the child. In making this assessment, the Commissioner would be able to take a range of factors into account, such as:
  - the occasion, context and content of the material;
  - the circumstances under which the material was placed on the social media site;
  - the risk of triggering suicide or life-threatening mental health issues for the child;
  - the age and characteristics of the child; and
  - any other matter which the Commissioner may consider relevant;
- the material would have to be on a participating social media site; and
- the material would have to have been placed on the participating social media site by a third party.

Q13 Are the nominated factors, the appropriate factors to be taken into account when determining whether the statutory test has been met? Should other factors be considered in this test?

Q14 Is the test of '**material targeted at and likely to cause harm to an Australian child**' appropriate?

If the material meets the statutory test for **material targeted at and likely to cause harm to an Australian child**, the Commissioner would have the options of:

- issuing a notice to the individual(s) that posted the material on the social media site to remove the material; and/or
- issuing a notice to the participating social media site to remove the material.

The Commissioner might issue a notice to an individual if the Commissioner considers that will be the quickest and most effective way of removing the material.

The Commissioner might issue a notice to the participating social media site, for example, if the individual that posted the content is not readily identifiable or if the applicable material has been shared by a number of individuals on the same social media site and a notice to the site will be the most efficient way of achieving rapid removal.

The notice to remove the material would set out required timeframes for the removal of material, and penalties for non-compliance.

Q15 What is an appropriate timeframe for material to be removed?

Penalties and enforcement

Where a participating social media site fails to comply with its obligation to maintain complaints handling and rapid removal arrangements (and maintain satisfactory performance of these arrangements), sanctions for non-compliance should apply. Sanctions would also apply to individuals who fail to comply with notices. The proposed scheme may include a range of lower and higher level penalties which require further consideration. Sanctions might include:

- the Commissioner issuing public statements about numbers of complaints received relating to participating social media sites, as well as publishing statements about non-compliance with notices to remove material;
- the Commissioner issuing formal warnings to individuals and participating social media sites;
- the Commissioner issuing infringement notices to individuals, which may include an appropriate fine. Careful consideration will be given to circumstances under which the Commissioner might serve an infringement notice to an individual under 18 years old;
- civil penalties for participating social media sites; and
- the Commissioner issuing public advice that a particular site is not safe for children to use.

The Government expects compliance with Australian laws by foreign companies that choose to operate within Australia. The Government also notes that some of the major social media sites have

issued public statements[28] that they will comply with the domestic laws of the countries within which they operate, particularly with regards to content removal. In considering the above options for penalties and enforcement, the Government notes that a range of factors may impact the effectiveness of enforcement mechanisms. For example, the proposed scheme may be quickly and simply enforceable against social media sites located in Australia. However, where a relevant social media site operator is not located, or does not have a sufficient presence, in Australia,[29] enforcement of the above regulatory measures is likely to be more difficult.

While many of the major social media sites do have some degree of Australian presence, for the most part, the Australian registered companies for these sites only have responsibility for subsidiary activities (such as advertising and sales support), and most sites operate their core business of providing social media services from overseas. Other emerging social media sites popular with Australian children do not have any Australian presence.

Most of the major social media sites have well-established complaints handling procedures that generally apply across all jurisdictions in which the sites operate. Therefore, compliance with these new proposed arrangements would involve an expansion of an existing function, rather than establishing an entirely new function. However, in the event that a pattern emerges of a participating social media site failing to comply with notices from the Commissioner to remove material, the Government would consider how penalties might be applied to entities that lack the requisite Australian presence.

The New Zealand scheme provides a safe harbour for online content hosts from civil and criminal liability under the proposed new regime (see Appendix C). The New Zealand safe harbour provision states that a content host is not liable for content they host, unless the content host has received a notice of complaint about the content, and fails to take reasonable steps to remove it. The aim of these provisions is to ensure that a content host cannot be held liable for content they host that is posted by another person, but which the host does not know about. This gives the online content host an incentive to have a complaints scheme and to comply with notices from the regulator. Consideration could be given to whether a similar safe harbour should be provided to social media sites under this option.

Q16 What would be the best way of encouraging regulatory compliance by participating social media sites that lack an Australian presence?[30]

[28] Peter Van der Veen, *Twitter to remove unlawful tweets: threat to free speech or the reality of internet business?*, 27 January 2012 and *Google follows Twitter: Country specific NTD to comply with local law*, 3 February 2012

[29] An Australian presence could include the registration of an Australian company incorporated in Australia, or the registration of a foreign company with the Australian Securities and Investments Commission under the *Corporations Act 2001* on the basis that it is carrying on business in Australia.

[30] In considering this question, readers may wish to review the ACMA's paper *Cross-border regulatory strategies; Case studies in regulatory practice for a networked economy and society*, which was released in October 2013. This paper makes a case for a mix of regulatory tools to ensure compliance with domestic regulatory measures. These include, but are not limited to, a range of domestic legal and industry tools

Q17 Should the proposed scheme offer safe harbour provisions to social media sites which have a complying scheme, and if so, what should they be?

Administration of proposed scheme

The legislation would provide the Commissioner with the capacity to:

- receive and assess complaints under the scheme;
- determine whether the scheme applies (that is, whether the material the subject of the complaint appeared on a participating social media site);
- determine whether the material the subject of the complaint meets the test for **material targeted at and likely to cause harm to an Australian child,** conducting any necessary investigation;
- if the material meets the test, issue a direction to remove the material;
- take enforcement action where a participating social media site fails to comply with the requirements of the scheme or where an individual posts material which is targeted at and likely to cause harm to an Australian child, including issuing warnings and infringement notices and instituting proceedings for injunctions or civil penalties for failure to comply with directions; and
- issue an annual report with statistics for each participating social media site on complaints received, the broad nature of complaints and generally how these were resolved.

The proposed scheme would not replace or inhibit the operation of the current Online Content Scheme under the *Broadcasting Services Act 1992*. Any online content which falls within the scope of the current Online Content Scheme would be dealt with under that scheme.

Legislative framework

The proposed scheme will be set out in legislation, which will provide a clear statutory framework and suitable powers to the Commissioner for administering the scheme.

Privacy

The proposed scheme would ensure that complainants are made aware of the way in which their personal information is collected and used to process complaints. Requirements under the *Privacy Act 1988* would be taken into consideration in drafting the legislation for the proposed scheme to ensure that personal information is handled appropriately.

(including education programs, taxation approaches, industry codes, industry and consumer levies and graduated response models), and also cross-border legal harmonisation.

Rights of appeal

Affected parties, including the individual who posted the material which was the subject of the complaint, would have a right of appeal to the Administrative Appeals Tribunal.

However, it is intended that the material should be removed in response to a notice. Any appeal would relate to allowing the material to be reinstated. In cases of material which is potentially harmful or distressing to a child, the scheme should favour the interests of the child, rather than the person seeking to publish the material.

Q18 Is merits review by the Administrative Appeals Tribunal the most appropriate review mechanism and if so, which parties and in relation to which types of decision is it appropriate? What are the alternatives?

Impact on business

A regulatory impact statement will be prepared following consultation with industry.

Q19 What do industry representatives consider are the estimated financial and administrative impacts of compliance with the proposed scheme? How are these estimated impacts derived?

Review of proposed scheme

The Department will review the proposed scheme three years after implementation.

3. Options for dealing with cyber-bullying under Commonwealth legislation

As outlined in the policy to *Enhance Online Safety for Children*, the Government is committed to examining existing Commonwealth legislation to determine whether to create a new, simplified cyber-bullying offence. While there are existing laws in Australia that cover such conduct, many people, especially minors, may not be aware that the existing laws may apply. It is also important that Australians clearly understand that cyber-bullying may constitute an offence; that any penalties are appropriate, especially when young people offend; and a broad range of sentencing options apply, particularly in instances where the offender is a minor.

There are existing provisions which arguably apply to such conduct. 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, in all the circumstances, menacing, harassing or offensive. This was introduced in 2005.[31] 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.

The existing offences under the Criminal Code are set out in Appendix B.

Commentary on the existing offence 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.

One of the outcomes of the National Bullying, Young People and the Law Symposium, which was held in July 2013, was the recommendation:

> All governments to consider the introduction of a specific, and readily understandable, criminal offence of bullying, including cyberbullying, involving a comparatively minor penalty to supplement existing laws which are designed to deal with more serious forms of conduct. In developing the above approaches, it is necessary to take into account:
>
> i the voices of children and human rights advocates
> ii summary offences that do not require proof of specific intent to cause harm
> iii appropriate penalties that in the case of children do not include incarceration.[32]

Three possible options for proceeding are described below. In considering these options, it is worth noting the age limit defences for children that generally apply to Commonwealth offences which are

[31] *Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Act (No.2) 2004*
[32] Recommendations of the *Bullying, Young People and the Law Symposium*, Australia,18-19 July 2013

set out in the Criminal Code at sections 7.1 and 7.2 (and mirrored in the *Crimes Act 1914* at sections 4M and 4N) to the effect that:

- a child under 10 years is not criminally responsible for an offence; and
- a child over 10 but under 14 years can only be criminally responsible for an offence if the child knows that his or her conduct is wrong (which is a factual test that the prosecution bears the onus of proving).

3.1. Options for a Commonwealth cyber-bullying offence

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

Some characteristics of the existing offence include that it:

- covers a broad 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 and 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.

Examples of prosecutions under this offence include:

- posting offensive pictures and comments on Facebook tribute pages for several dead or missing children *(R v Hampson [2011] QCA 132)*;
- posting menacing messages on Facebook *(Agostino v Cleaves [2010] ACTSC 19)*; and
- sending repeated menacing emails *(R v Ogawa [2009] QCA 307)*.

Cyber-bullying was considered at the Standing Council on Law and Justice meeting on 5 October 2012. At that time, Attorneys-General agreed that current Commonwealth, state and territory laws provide appropriate coverage of serious instances of cyber-bullying.[33]

However, some criticisms of the current offence are that:

[33] Communiqué, Standing Council on Law and Justice, Australia, 5 October 2012

- the existing offence is too general and not designed to specifically cover cyber-bullying;
- the size of the maximum penalty is disproportionately large for most cyber-bullying cases, particularly for application to minors, and an offence with a comparatively minor maximum penalty would provide a better option for less serious forms of conduct; and
- the existing offence is worded in a way that people, particularly minors, would not understand – many young people do not realise that cyber-bullying can be a criminal offence.

It may be that more needs to be done to raise awareness about the existing law and its application to cyber-bullying. This may increase the effectiveness of the existing law in deterring growing levels of cyber-bullying. Consideration could be given to providing better education and messaging to students, parents and teachers and law enforcement agencies about the current offences and the legal consequences of cyber-bullying.

The Attorney-General's Department is working with CrimTrac and the Australian Crime Commission to develop the Australian Cybercrime Online Reporting Network (ACORN), in consultation with law enforcement agencies. The ACORN is an internet based system that will:

- receive cybercrime reports from members of the public;
- provide general and targeted educational advice on cybercrime; and
- refer certain reports to law enforcement agencies for further consideration.

It is expected that the ACORN will be operational in the second half of 2014.

Q20 In light of the Government's proposed initiatives targeting cyber-bullying set out in Chapters 1 and 2; do the current criminal laws relating to cyber-bullying require amendment?

Q21 Is the penalty set out in section 474.17 of the Criminal Code appropriate for addressing cyber-bullying offences?

Option 2 – Create a separate cyber-bullying offence covering conduct where the victim is a minor (under 18 years), with a lesser maximum penalty such as a fine

Consideration could be given to creating a new separate cyber-bullying offence which covers conduct where the victim is a minor (under 18 years) with a lesser maximum penalty, such as a fine. Such an offence could be based on section 474.17 of the Criminal Code. This would still allow recourse to the existing offence for particularly serious incidents.

If passed into law, New Zealand's *Harmful Digital Communications Bill*[34] will establish the offence of causing harm by posting a digital communication, and provides that a person found to have committed this offence is liable to imprisonment for up to 3 months, or a fine not exceeding $2,000.

[34] *Harmful Digital Communications Bill*, New Zealand Parliament, 5 November 2013

The criminal offence proposed in the bill is outlined at Appendix C. Lesser penalties could also include counselling, restorative justice, community-based orders and probation. Under the *Crimes Act 1914* (Cth), judges sentencing federal offenders are able to rely on certain State and Territory alternative sentencing options, including community service orders, work orders, sentence of periodic detention and attendance centre orders. It should be noted that these alternatives exist at the state and territory level, and vary across jurisdictions.

The benefits of creating a mid-range cyber-bullying offence could 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.

Limitations of this option may include:

- the possibility that it may over-extend to behaviour which should not be treated as a criminal offence, and encourage over-reporting of incidents;
- a potential large increase in reporting of cyber-bullying to police, who may not have the resources to respond in many cases;
- 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 also cause confusion regarding the application of the existing offence.

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

3.2. Options for a Commonwealth civil penalty regime

Option 3 – Create a separate civil enforcement regime to deal with cyber-bullying modelled on the New Zealand 'Approved Agency' approach

New Zealand proposal

On 5 November 2013, the New Zealand Government introduced the *Harmful Digital Communications Bill* into Parliament, which proposed a new criminal offence for causing harm by posting digital communication.[35] The criminal offence proposed in the bill was discussed above in Option 2 and is outlined at Appendix C.

[35] *Harmful Digital Communications Bill*, New Zealand Parliament, 5 November 2013

In addition to creating a criminal offence, the New Zealand bill provides for a civil enforcement regime. Under the New Zealand regime, a person complaining of being the subject of a harmful digital communication may make a complaint to the 'Approved Agency' (the Children's e-Safety Commissioner could perform this role in Australia). Complaints can also be made by the parent or guardian, or school principal, of the person the subject of the communication.

Under the New Zealand regime, the Approved Agency will have the following responsibilities:

- receive and assess complaints about harm caused to persons by digital communications;
- use negotiation, mediation, and persuasion (as appropriate) to resolve complaints; and
- investigate complaints.

If the Approved Agency has had the opportunity to consider the matter, and it has not been satisfactorily resolved, the complainant can go to court and seek various orders including to take down the material. Orders can be made against both the person who posted the material and the online content host. Appendix C contains a full description of the civil enforcement regime in the New Zealand bill.

Australian proposal

In an Australian context, the Government is considering the possible introduction of a similar civil penalty regime to target cyber-bullying behaviour. The Children's e-Safety Commissioner could be given the power to receive and assess complaints about cyber-bullying, investigate those complaints, and facilitate negotiation and mediation between the parties to a complaint. The Commissioner would have the discretion to only exercise these powers for complaints about conduct that:

- occurs through electronic communication to, or relating to, an Australian child; and
- a reasonable person would regard as being, in all the circumstances, likely to cause harm to the child (with 'harm' being defined similarly to the New Zealand bill, to mean serious emotional distress).

In circumstances where the negotiations/mediation activities do not result in a satisfactory outcome, the Commissioner would be able to make a decision about the dispute, and issue notices to individuals who are a party to the dispute to:

- remove, take down or delete material;
- cease the specific conduct concerned; or
- other actions that the Commissioner thinks appropriate to prevent the cyber-bullying from continuing.

A civil penalty provision of failing to comply with a notice from the Commissioner would attach to non-compliance. The Commissioner would have the power to issue infringement notices for failure to comply (see further discussion of infringement notices, below).

This civil regime could parallel the proposed scheme for rapid removal of harmful material related to a child from social media sites (set out in Chapter 2), with the following key differences:

- it would not be restricted to material posted on participating social media sites, but would instead capture a wider range of electronic communication (such as email and SMS);

- the Commissioner's ability to facilitate a range of activities with the individuals involved in the cyber-bullying dispute, such as mediation sessions, allows the parties to participate in the dispute resolution and assist in reaching a mutually beneficial outcome; and
- the Commissioner would have a wider range of powers in relation to issuing notices to individuals – whilst the proposed scheme under Chapter 2 only allows individuals to be issued with notices to remove material from the social media site, under this option the Commissioner could issue notices applying to a wider range of conduct that contributes to the alleged cyber-bullying.

The Commissioner would receive cyber-bullying complaints either from school principals or police. In a limited range of circumstances, the Commissioner may also receive complaints directly from the public.

Where appropriate, the Commissioner would also have the power to refer matters to KidsHelpline (or another relevant organisation) where a child requires urgent counselling or support; and refer the matter to police where, after investigation, the Commissioner considers the nature of the complaint warrants a law enforcement response.

Another issue that would need to be addressed is appropriate resourcing of the Commissioner to undertake this role. There may be a case for transferring relevant resources from other agencies to the Commissioner to undertake this role.

Infringement notice scheme

The penalties under the infringement notice scheme should be high enough to dissuade and attract parental attention, but not so high that it leads people to contest the matter as a preferable option (perhaps a $1,000 fine). A person who receives an infringement notice would have options for payment or contesting the notice (perhaps in the Administrative Appeals Tribunal or the Federal Circuit Court).

The advantages of implementing an infringement notices scheme could include:

- a faster, more effective process for dealing with cyber-bullying complaints, by avoiding the delays of court processes;
- increased deterrence effect leading to a reduction in the overall level of cyber-bullying;
- reduced burden on the legal system; and
- reduced legal impact and trauma on minors.

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

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

Appendix A

Current Australian Government online safety programmes and resources

Programmes and resources	Agency
The ***Cybersafety Help Button*** is a free downloadable resource providing a one-stop-shop for online safety information and advice. It provides users with the option to talk to someone about online issues that are of concern, report inappropriate online content or behaviour, and learn about good online safety practices.	Department of Communications
The ***Easy Guide to Socialising Online*** provides information about the online safety features of different social media sites, search engines and online games. The Easy Guide provides clear, step-by-step instructions on how to adjust privacy settings, as well as site specific advice on how to report cyber-bullying, online abuse and harmful content.	Department of Communications
The ***Australian Government Cybersafety Help Facebook*** page promotes online safety resources and initiatives. The page provides an opportunity for users to discuss online safety issues and share information.	Department of Communications
The ***Australian Children's Cybersafey and E-security Project*** is a research project administered by the Department of Communications into changes in awareness and behaviour in relation to online safety and security risks relevant to children.	Department of Communications
The ***Online Content Scheme***, currently administered by the ACMA, is set out in the *Broadcasting Services Act 1992* and provides a complaints-based scheme for offensive and illegal online content with power to issue take-down notices.	Australian Communications and Media Authority
The ACMA's ***Cybersmart*** programme is a national online safety and security education programme designed to encourage participation in the digital economy by providing information and education that empowers children to be safe online.	Australian Communications and Media Authority
Other initiatives within the ACMA's suite of online safety initiatives, such as ***Tagged***, which is a video that deals with issues of cyber-bullying, sexting and digital reputation; ***Connect.ed***, which is a professional online safety development programme; ***Zippep's Astro Circus***, which is an online cyber safety game that guides children aged five to seven in having safe online experiences; as well as a blog, Twitter account and Facebook page titled ***The Cloud: Dream On***, which provides online safety	Australian Communications and Media Authority

information for teens.	
The ACMA's ***research programme***, which conducts a range of research projects into the use of the internet by children and young people, including major quantitative and qualitative studies of the way children and young people use the internet and manage online risks; research to update its own suite of online safety material and programmes for parents and carers to evaluate key educational resources; and longitudinal studies of children's media and communications use.	Australian Communications and Media Authority
The Australian Federal Police's ***ThinkUKnow*** programme provides online safety information, advice and tools for youth, parents, carers and teachers through schools and organisations across Australia using a network of accredited trainers. The *ThinkUKnow* website has a 'Report Abuse' function which is used to report online grooming behaviour.	Australian Federal Police
The Line campaign aims to prevent violence against women by connecting with Australian teenagers and communicating respectful relationship information (including online). The Line campaign is an initiative under the National Plan to Reduce Violence against Women and their Children 2010 – 2022.	Department of Social Services
The ***Safe Schools Hub*** is a one-stop shop for information and resources on safe school strategies to assist teachers, students and parents. The Hub provides the tools and knowledge that enables all members of the school community to support students who are impacted by anti-social behaviour, including cyber-bullying.	Department of Education
Bullying No Way! is managed by the Safe and Supportive School Communities (SSSC) Working Group. The SSSC includes education representatives from the Commonwealth and all states and territories, as well as national Catholic and independent schooling representatives. Members work together to create learning environments where every student and school community member is safe, supported, respected and valued.	Commonwealth, state and territory education authorities
The ***BackMeUp*** campaign encourages young people to support their friends targeted by cyber-bullying.	Australian Human Rights Commission

Appendix B

Current offences in the Criminal Code Act 1995 (Cth)

Section 474.15 - Using a carriage service to make a threat

Threat to kill

1. A person (the ***first person***) is guilty of an offence if:
   (a) the first person uses a carriage service to make to another person (the ***second person***) a threat to kill the second person or a third person; and
   (b) the first person intends the second person to fear that the threat will be carried out.

   Penalty: Imprisonment for 10 years.

Threat to cause serious harm

2. A person (the ***first person***) is guilty of an offence if:
   (a) the first person uses a carriage service to make to another person (the ***second person***) a threat to cause serious harm to the second person or a third person; and
   (c) the first person intends the second person to fear that the threat will be carried out.

   Penalty: Imprisonment for 7 years.

Actual fear not necessary

3. In a prosecution for an offence against this section, it is not necessary to prove that the person receiving the threat actually feared that the threat would be carried out.

Definitions

4. In this section:

   fear includes apprehension.
   threat to cause serious harm to a person includes a threat to substantially contribute to serious harm to the person.

Section 474.17 - Using a carriage service to menace, harass or cause offence

1. A person is guilty of an offence if:
   (a) the person uses a carriage service; and
   (b) the person does so in a way (whether by the method of use or the content of a communication, or both) that reasonable persons would regard as being, in all the circumstances, menacing, harassing or offensive.

   Penalty: Imprisonment for 3 years.

2. Without limiting subsection (1), that subsection applies to menacing, harassing or causing offence to:
   (a) an employee of an NRS provider; or
   (b) an emergency call person; or
   (c) an employee of an emergency service organisation; or
   (d) an APS employee in the Attorney-General's Department acting as a National Security Hotline call taker.

Appendix C

New Zealand's *Harmful Digital Communications Bill* (criminal offence and civil enforcement regime)

On 5 November 2013, the New Zealand Government introduced the Harmful Digital Communications Bill into parliament. The Bill implements the Government's decisions on addressing harmful digital communications, which were largely based on the Law Commission's 2012 Ministerial Briefing paper Harmful Digital Communications: The adequacy of the current sanctions and remedies.

Harmful digital communications, cyber-bullying, and digital harassment can take many forms, including communicating through emails, texts, blog sites, forums, and social media sites such as Facebook and Twitter.

Modern technology has therefore provided an outlet for a unique form of harassment with its own challenges. This is due to the:

- ubiquity and ease of access to technology in modern life;
- ease and speed of dissemination and the potential to go "viral" to a global audience;
- persistence of the information and difficulty in removing it; and
- facility for anonymity.

The victims of harmful digital communications are often children and young people, who are particularly vulnerable and require appropriate protections.

Purpose and overview of the Bill

The purpose of this Bill is to mitigate the harm caused to individuals by digital communications and to provide victims of harmful digital communications with a quick and efficient means of redress.

To achieve that purpose, this Bill:

- creates a new civil enforcement regime to quickly and effectively deal with harmful digital communications;
- creates new criminal offences to deal with the most serious harmful digital communications; and
- makes some small amendments to existing legislation to clarify their application to digital communications and cover technological advances.

Civil enforcement regime

The key policy objectives of the new civil enforcement regime are ensuring:

- effective and accessible remedies for victims of harmful digital communications;
- the response is proportionate to the harm; and
- remedies are cost effective and quick.

This Bill sets out 10 new communication principles to guide the functions of the court and the Approved Agency. The principles are:

1. A digital communication should not disclose sensitive personal facts about an individual.
2. A digital communication should not be threatening, intimidating, or menacing.
3. A digital communication should not be grossly offensive to a reasonable person in the complainant's position.
4. A digital communication should not be indecent or obscene.
5. A digital communication should not be part of a pattern of conduct that constitutes harassment.
6. A digital communication should not make a false allegation.
7. A digital communication should not contain a matter that is published in breach of confidence.
8. A digital communication should not incite or encourage anyone to send a message to a person with the intention of causing harm to that person.
9. A digital communication should not incite or encourage another person to commit suicide.
10. A digital communication should not denigrate a person by reason of his or her colour, race, ethnic or national origins, religion, gender, sexual orientation, or disability.

The new civil enforcement regime provides for initial complaints about harmful digital communications to be made to an Approved Agency. The Approved Agency may investigate a complaint and attempt to resolve it by negotiation, mediation, and persuasion.

Where the Approved Agency cannot resolve the complaint, an individual (which includes a person who alleges that he or she has suffered harm, a parent or guardian, a principal of an educational establishment, the Police or the Chief Coroner) may make an application to the District Court for a number of civil orders against a defendant and an online content host. The court may also make a declaration that a communication breaches a communication principle. While not a mandatory authority, this would have significant persuasive power in relation to website hosts or ISPs operating outside New Zealand jurisdiction.

The court will have jurisdiction over all forms of digital communication, be able to use an expert technical adviser to ensure any remedies are technically achievable and appropriate and operate according to rules that will facilitate speedy, cheap, and informal justice.

Orders that may be made by court

1. The District Court may, on an application, make 1 or more of the following orders against a defendant:

   (a) an order to takedown material;
   (b) an order that the defendant cease the conduct concerned;
   (c) an order that the defendant not encourage any other persons to engage in similar communications towards the person specified in section 10(1)(a);
   (d) an order that a correction be published;
   (e) an order that a right of reply be given to the person specified in section 10(1)(a);
   (f) an order that an apology be published.

2. The District Court may, on an application, make 1 or more of the following orders against an online content host:

   (a) an order to take down or disable public access to material;
   (b) an order that the identity of the author of an anonymous communication be released;
   (c) an order that a correction be published;
   (d) an order that a right of reply be given to the person specified in section 10(1)(a).

3. The court may also do 1 or more of the following:

   (a) make a direction applying an order provided for in subsection (1) or (2) to other persons specified in the direction, if there is evidence that those others have been encouraged to engage in harmful digital communications towards the person specified in section 10(1)(a);
   (b) make a declaration that a communication breaches a communication principle;
   (c) order that the names of any specified parties be suppressed.

4. In deciding whether or not to make an order, and the form of an order, the court must take into account the following:

   (a) the content of the communication and the level of harm caused by it;
   (b) the purpose of the communicator, in particular whether the communication was intended to cause harm;
   (c) the occasion, context, and subject matter of the communication;
   (d) the extent to which the communication has spread beyond the original parties to the communication;
   (e) the age and vulnerability of the victim;
   (f) the truth or falsity of the statement;
   (g) whether the communication is in the public interest;
   (h) the conduct of the defendant, including any attempt by the defendant to minimise the harm caused;
   (i) the conduct of the victim or complainant;
   (j) the technical and operational practicalities, and the costs, of an order.

5. In doing anything under this section, the court must act consistently with the rights and freedoms contained in the New Zealand Bill of Rights Act 1990.

Criminal offences

In addition to a new offence of failing to comply with an order of the court, this Bill creates further offences to deal with the most serious forms of harmful digital communications, including an offence of posting a harmful digital communication with the intention to cause harm.

Causing harm by posting digital communication

1. A person commits an offence if:

   (a) the person posts a digital communication with the intention that it cause harm to a victim; and
   (b) posting the communication would cause harm to an ordinary reasonable person in the position of the victim; and
   (c) posting the communication causes harm to the victim.

2. In determining whether a post would cause harm, the court may take into account any factors it considers relevant, including:

   (a) the extremity of the language used;
   (b) the age and characteristics of the victim;

(c) whether the digital communication was anonymous;
(d) whether the digital communication was repeated;
(e) the extent of circulation of the digital communication;
(f) whether the digital communication is true or false;
(g) the context in which the digital communication appeared.

3. A person who commits an offence against this section is liable to imprisonment for a term not exceeding 3 months or a fine not exceeding $2,000.

4. In this section:

intimate visual recording:

(a) means a visual recording (for example, a photograph, videotape, or digital image) that is made in any medium using any device with or without the knowledge or consent of the person who is the subject of the recording, and that is of:
  (i) a person who is in a place which, in the circumstances, would reasonably be expected to provide privacy, and that person is:
    (A) naked or has his or her genitals, pubic area, buttocks, or female breasts exposed, partially exposed, or clad solely in undergarments; or
    (B) engaged in an intimate sexual activity; or
    (C) engaged in showering, toileting, or other personal bodily activity that involves dressing or undressing; or
  (ii) a person's naked or undergarment-clad genitals, pubic area, buttocks, or female breasts which is made:
    (A) from beneath or under a person's clothing; or
    (B) through a person's outer clothing in circumstances where it is unreasonable to do so.

(b) includes an intimate visual recording that is made and transmitted in real time without retention or storage in:
  (i) a physical form; or
  (ii) an electronic form from which the recording is capable of being reproduced with or without the aid of any device or thing.

posts a digital communication:

(a) means transfers, sends, posts, publishes, disseminates, or otherwise communicates by means of a digital communication any information, whether truthful or untruthful, about the victim; and
(b) includes publishing an intimate visual recording of another person; and
(c) includes an attempt to do anything referred to in paragraph (a) or (b).

victim means the person who is the target of the conduct elicited by the posted digital communication.

Safe harbour provisions

This Bill also clarifies the law relating to the liability of internet content hosts for content they host but which is posted by third parties. The purpose of this is to ensure that a content host cannot be held liable for content they host that is posted by another person, but which the host does not know about.

This Bill contains a safe harbour provision stating that a content host is not liable for content they host, unless the content host has received a notice of complaint about the content, and fails to take reasonable steps to remove it.

The protection provided by the safe harbour does not apply if:

- a content host does not provide an easily accessible mechanism for users to report such content to them or
- the provision is inconsistent with the express provisions of another enactment relating to the responsibilities of an online content host for content posted by others.