2013-2014

THE PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA

HOUSE OF REPRESENTATIVES

ENHANCING ONLINE SAFETY FOR CHILDREN BILL 2014

ENHANCING ONLINE SAFETY FOR CHILDREN (CONSEQUENTIAL AMENDMENTS) BILL 2014

EXPLANATORY MEMORANDUM

(Circulated by authority of the Minister for Communications,
the Hon. Malcolm Turnbull MP)

ENHANCING ONLINE SAFETY FOR CHILDREN BILL 2014

ENHANCING ONLINE SAFETY FOR CHILDREN (CONSEQUENTIAL AMENDMENTS) BILL 2014

OUTLINE

These bills implement Australian Government election commitments to enhance online safety for children, including:

- establishing a Children's e-Safety Commissioner (Commissioner) to take a national leadership role in online safety for children; and
- implementing an effective complaints system, backed by legislation that will get harmful cyber-bullying material targeted at an Australian child down quickly from large social media sites.

The bills were developed following substantial public and stakeholder consultation, including consideration of more than 80 submissions received in response to the public discussion paper 'Enhancing Online Safety for Children' released in January 2014.

Enhancing Online Safety for Children Bill 2014

The Enhancing Online Safety for Children Bill 2014 (the Online Safety Bill) provides for:

- establishing the Children's e-Safety Commissioner and sets out the Commissioner's functions and powers;
- a complaints system for cyber-bullying material targeted at an Australian child;
- a 2-tiered scheme for the rapid removal from large social media services of cyber-bullying material targeted at an Australian child;
- a mechanism for the Commissioner to give end-user notices to require a person who posts cyber-bullying material targeted at an Australian child to remove the material, refrain from posting further material or apologise to the child for posting the material;
- enforcement mechanisms for the Commissioner;
- administrative provisions relating to the Commissioner;
- the establishment of the Children's Online Safety Special Account to fund the Commissioner's activities;
- enabling the Commissioner to disclose information in specified circumstances; and
- other miscellaneous provisions.

Children's e-Safety Commissioner

Part 2 of the Online Safety Bill establishes the Commissioner and sets out the Commissioner's functions and powers. The Commissioner will be an independent

statutory office within the Australian Communications and Media Authority (ACMA). A key function of the Commissioner will be to administer a complaints system for cyber-bullying material targeted at an Australian child.

Other functions of the Commissioner will include promoting online safety for children, coordinating relevant activities of Commonwealth Departments, authorities and agencies, supporting, conducting, accrediting and evaluating educational and community awareness programs, making grants and advising the Minister. The Commissioner will also have the function of administering the online content scheme set out in Schedules 5 and 7 to the *Broadcasting Services Act 1992* (BSA) that was previously administered by the ACMA and is being transferred to the Commissioner without substantive amendment.

Complaints system

Part 3 of the Online Safety Bill establishes a complaints system for cyber-bullying material targeted at an Australian child. Complaints will be able to be made to the Commissioner by an Australian child or by a parent or guardian of the child. Other responsible persons will also be able to make a complaint on behalf of an Australian child, if the child authorises them to do so.

The Commissioner will have the power to investigate complaints and conduct such investigations as the Commissioner thinks fit.

Social media services

Part 4 of the Online Safety Bill establishes a 2-tiered scheme for the rapid removal from large social media services of cyber-bullying material targeted at an Australian child.

Division 1 of Part 4 sets out a statement of Parliamentary expectations that each social media service will comply with certain basic online safety requirements, those being that a social media service has:

- terms of use that prohibit the posting of cyber-bullying material;
- a complaints scheme under which end-users of the service can seek to have material that breaches the service's terms of use removed; and
- a contact person for the Commissioner to deal with.

The Commissioner will have the role of communicating that expectation to social media service providers as far as practicable.

Tier 1 social media services

Division 2 of Part 4 provides for tier 1 social media services. The provider of a social media service will be able to apply to the Commissioner for declaration of the service as a tier 1 social media service (tier 1 service). The Commissioner will be required to make such a declaration if satisfied that the service complies with the basic online safety requirements and the service is not a tier 2 social media service.

The Commissioner will have the power to request that the provider of a tier 1 service remove cyber-bullying material targeted at an Australian child within 48 hours where the Commissioner receives a complaint that the material was not removed within

48 hours (or such longer period as the Commissioner allows) following a complaint made under the service's complaints scheme.

There will be no direct enforcement measures in relation to tier 1 services. However, if a tier 1 service repeatedly fails to comply with requests to remove material over a 12 month period, or the Commissioner is satisfied that the service does not comply with the basic online safety requirements, the Commissioner may revoke the service's tier 1 status.

Tier 2 social media services

Division 3 of Part 4 provides for tier 2 social media services (tier 2 services). These services are subject to direct regulation and accordingly are declared by the Minister, following a recommendation from the Commissioner, by a legislative instrument subject to Parliamentary disallowance.

The Commissioner must not make a recommendation that a social media service be declared a tier 2 service if the service is a tier 1 service. The Commissioner also must not make a recommendation unless satisfied that the service is a large social media service or the provider of the service has requested tier 2 status. In deciding whether to make a recommendation, the Commissioner must have regard to certain matters, including whether the service complies with the basic online safety requirements, whether the service has failed to apply for tier 1 status or has had tier 1 status revoked.

The Commissioner will have the power to give a social media service notice to the provider of a tier 2 service requiring the provider to remove cyber-bullying material targeted at an Australian child within 48 hours where the Commissioner receives a complaint that such material on the tier 2 service was not removed within 48 hours (or such longer period as the Commissioner allows) following a complaint made under the service's complaints scheme.

A person who fails to comply with a social media service notice may be subject to a civil penalty. Other enforcement options will be available in the form of enforceable undertakings and injunctions.

The Commissioner will maintain registers of tier 1 and 2 social media services.

The Commissioner will also be able to publish statements about non-compliant social media services under Division 4 of Part 4 in respect of social media services failing to comply with the basic online safety requirements, failing to comply with a request for removal of cyber-bullying material, or failing to comply with a social media service notice.

End-user notices

Part 5 of the Online Safety Bill enables the Commissioner to give an end-user notice to a person who posts cyber-bullying material targeted at an Australian child requiring the person to take all reasonable steps to ensure the removal of the material, refrain from posting further material targeted at the child, or apologise to the child for posting the material.

An injunction will be able to be sought from the Federal Circuit Court for a failure to comply with an end-user notice.

Other provisions

Part 6 of the Online Safety Bill adopts enforcement arrangements set out in the *Regulatory Powers (Standard Provisions) Act 2014* in respect of civil penalties, enforceable undertakings and injunctions for the purposes of the Online Safety Bill.

Part 7 of the Online Safety Bill sets out administrative provisions relating to the Commissioner, including provisions relating to appointment, employment terms and conditions, supplementary powers, delegation of functions and powers, annual report, requirements on the ACMA to assist the Commissioner and ministerial directions.

Part 8 of the Online Safety Bill establishes the Children's Online Safety Special Account which will be used to fund the Commissioner's activities.

Part 9 of the Online Safety Bill enables the Commissioner to disclose information in certain circumstances. This Part will enable the Commissioner to disclose information to teachers or school principals to assist in the resolution of complaints made under the Online Safety Bill, which may be particularly important in cases of cyber-bullying among school children. Similarly, the Commissioner may disclose information to a parent or guardian of an Australian child, who may need to be informed to assist in the resolution of a complaint made under the Online Safety Bill.

Part 10 of the Online Safety Bill sets out other miscellaneous provisions, including provisions in relation to merits review of decisions, protections from civil and criminal proceedings and liability for damages, referral of matters to law enforcement agencies and the power for the Minister to make legislative rules.

Enhancing Online Safety for Children (Consequential Amendments) Bill 2014

The Enhancing Online Safety for Children (Consequential Amendments) Bill 2014 (the Consequential Amendments Bill) deals with consequential matters arising from the enactment of the Online Safety Bill.

Schedule 1 to the Consequential Amendments Bill contains amendments to the BSA to:

- give the Commissioner information gathering powers similar to those currently possessed by the ACMA under Part 13 of the BSA;
- change references in Schedules 5 and 7 to the BSA from the ACMA to the Commissioner to reflect the transfer of administrative responsibility for the Online Content Scheme in those Schedules to the Commissioner; and
- make minor consequential amendments to provisions in those Schedules.

Schedule 2 to the Consequential Amendments Bill contains consequential amendments to other Acts arising from the establishment of the Commissioner.

Schedule 3 to the Consequential Amendments Bill contains transitional provisions relating to the transfer of administrative responsibility for the Online Content Scheme in Schedules 5 and 7 of the BSA to the Commissioner.

FINANCIAL IMPACT STATEMENT

The Commissioner will be established as an independent statutory office within the ACMA. Funding for the Commissioner's activities will be allocated to the Children's Online Safety Special Account (the Special Account) established under Part 8 of the Online Safety Bill.

The funding to be allocated will be $6.7 million in 2014-15 and approximately $11 million per annum thereafter.

The Commissioner's approval will be required for any expenditure from the Special Account.

The bills will not otherwise have a significant impact on Commonwealth expenditure or revenue.

STATEMENT OF COMPATIBILITY WITH HUMAN RIGHTS

Prepared in accordance with Part 3 of the Human Rights (Parliamentary Scrutiny) Act 2011

Enhancing Online Safety for Children Bill 2014

Enhancing Online Safety for Children (Consequential Amendments) Bill 2014

These bills are compatible with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011*.

Overview of Bills

Certain material may be considered 'cyber-bullying material targeted at an Australian child' under clause 5 of the *Enhancing Online Safety for Children Bill 2014* (Online Safety Bill), if the material satisfies the following conditions:

(a) the material is provided on a social media service or relevant electronic service;

(b) an ordinary reasonable person would conclude that it is likely that the material was intended to have an effect on a particular Australian child;

(c) an ordinary reasonable person would conclude that the material would be likely to have the effect on the Australian child of seriously threatening, seriously intimidating, seriously harassing or seriously humiliating the Australian child;

(d) such other conditions (if any) as are set out in the legislative rules.

If all of these conditions are satisfied, under paragraphs 5(1)(d) – (e) of the Online Safety Bill, the material is cyber-bullying material targeted at the Australian child and the Australian child is the target of that material.

A recent study has estimated that, over a 12 month period, around 20 percent of young Australians aged 8–17 will have been the victims of cyber-bullying, with the number of children and young people estimated to have been affected being 463,000.[1] This study observed that the prevalence of cyber-bullying has rapidly increased since it first emerged as a behaviour, and suggested that this might be a result of the following factors:

- the increasing numbers of children and young people having access to the internet and to smartphones and their increasing propensity to use online methods to communicate
- the perception that cyber-bullying is more difficult to detect and that bullies are less likely to face consequences for cyber-bullying and lack awareness of the potential effects of cyber-bullying on victims.

---

[1] 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.

Like ‘traditional’ bullying, cyber-bullying can have lasting effects on individuals and their families, including self-esteem, mental health, depression, anxiety and suicidal ideation.

The Online Safety Bill establishes the Children’s e-Safety Commissioner (the Commissioner). The Commissioner will have a range of functions and powers, including: promoting online safety for children, promoting and conducting research in relation to online safety for children, and making grants of financial assistance in relation to online safety for children.

In addition, the Online Safety Bill will establish a system under which persons will be able to make complaints about cyber-bullying material that targets a particular Australian child, and the Commissioner will be able to investigate those complaints. After conducting such an investigation, if the material is provided on particular kinds of services known as ‘social media services’ or ‘relevant electronic services’, the Commissioner will be able to require the end-user who posted the material to take all reasonable steps to ensure the removal of the material, to refrain from posting further cyber-bullying material for which that person is the target, and/or to apologise to the person for posting the material. This is known as an ‘end-user notice’. In the case of material that is posted to a social media service, depending on the type of social media service to which it is posted, the Commissioner will also be able to either request or require the provider of the social media service to remove the material from its service. This is known as a ‘social media service notice’.

The Online Safety Bill contains provisions dealing with the enforcement of these requirements. If a person fails to comply with a requirement under an end-user notice, the Commissioner will be able to issue a formal warning. If the provider of a social media service fails to comply with a requirement under a social media service notice, they will be liable to pay a penalty of 100 penalty units. The Commissioner will additionally be able to accept an enforceable undertaking from such a provider. In the case of either a requirement under an end-user notice or a requirement under a social media service notice, the Commissioner will be able to seek an injunction to ensure compliance with the notice. In each case, enforcement is governed by the standard provisions that are contained in the *Regulatory Powers (Standard Provisions) Act 2014*.

The Online Safety Bill also deals with associated administrative matters.

The Consequential Amendments Bill makes consequential amendments to a number of other enactments to ensure smooth implementation of the Online Safety Bill.

Human rights implications

The principal human rights that the Online Safety Bill engages are:

- the right to freedom of expression, which is recognised by the Convention on the Rights of the Child (the CROC) as well as by the International Covenant on Civil and Political Rights (the ICCPR) and the Convention on the Rights of Persons with Disabilities (the CRPD)
- the right to protection from unlawful attacks on honour and reputation, which is recognised by the CROC
- the right to privacy, which is recognised by the CROC, the ICCPR and the CRPD;

- rights that ensure certain minimum guarantees in criminal proceedings, which is recognised by the ICCPR, the CROC and the CRPD.

The Consequential Amendments Bill deals with a range of facilitative technical amendments to legislation, and does not engage any human rights.

These rights, and how they are impacted by the Online Safety Bill, are discussed in more detail below.

Freedom of expression

Rights relating to freedom of expression are recognised and protected by Articles 12 and 13 of the CROC.

Paragraph 1 of Article 12 of the CROC recognises the right of a child who is capable of forming his or her own views to express those views freely in all matters affecting the child. Paragraph 2 of that Article recognises the right of a child to be heard in judicial and administrative proceedings that affect the child.

Paragraph 1 of Article 13 of the CROC recognises the right of a child to freedom of expression. Paragraph 2 of that Article recognises that the exercise of this right may be subject to certain restrictions. The CROC limits the types of restrictions that may be imposed, relevantly, to such restrictions as are provided by law and are necessary either for respect of the rights or reputations of others.

Other human rights treaties recognise similar rights, for example, Article 19 of the ICCPR and Article 21 of the CRPD. The comments below apply equally to these other treaties.

The guarantee of freedom of expression is considered to be fundamental to a free and democratic society. It is recognised as extending to protecting expression that may be regarded as offensive. Accordingly, restrictions must not be overbroad, must be proportionate, and must be the least intrusive instrument amongst those which might achieve their protective function.

Many provisions of the Online Safety Bill are consistent with these human rights. For example, the Online Safety Bill permits a child who is the target of cyber-bullying to make a complaint about cyber-bullying material, either themselves (subclause 18(1)) or through a representative (subclause 18(2)). The ordinary rules of natural justice will apply in relation to any investigations that are carried out under the Online Safety Bill, and hence both the child at whom the cyber-bulling material is targeted, as well as the end-user who provided the material, will have a right to be heard in any proceedings under or that relate to the Online Safety Bill. As a result, to that extent, the Online Safety Bill is consistent with the rights recognised by Article 12 of the CROC.

Further, subclause 100(1) of the Online Safety Bill provides that the Bill does not apply to the extent (if any) that it would impinge the constitutional doctrine of implied freedom of political communication. This ensures that the Online Safety Bill is consistent with the rights to freedom of expression as it relates to political communication.

However, protecting children from cyber-bullying by addressing and preventing some of the worst instances of cyber-bullying is a policy objective that is intrinsically restrictive of freedom of expression. Because of that, several provisions of the Online Safety Bill are restrictive of freedom of expression.

In particular, the Online Safety Bill restricts the exercise of the right to freedom of expression of an end-user who wishes to exercise this right by providing cyber-bullying material. If the cyber-bullying material is provided on a 'social media service', the end-user's right to freedom of expression so far as it relates to provision of cyber-bullying material could be restricted by the provider of the social media service being requested or required, under Part 4 of the Online Safety Bill, to remove the material from the service. If the cyber-bullying material is posted to a 'social media service' or a 'relevant electronic service', the end-user's right to freedom of expression, so far as it relates to provision of cyber-bullying material, could be restricted further by their being given an 'end-user notice' under Part 5 of the Online Safety Bill. This notice would require the end-user to take all reasonable steps to ensure the removal of the material, to refrain from posting cyber-bullying material targeting that child, and/or to apologise to the person at whom the material was targeted for posting the material.

The Online Safety Bill is, nevertheless, consistent with these human rights treaties.

To the extent the Online Safety Bill restricts the end-user's right to freedom of expression, the restriction is considered to be within the allowable restrictions that may be imposed under paragraph 2 of Article 13 of the CROC. As required by this paragraph, the restriction would be provided by law, the relevant law being the Online Safety Bill. Also as required by this paragraph, the restriction is considered necessary for respect of the rights or reputations of the child at whom the cyber-bullying material is targeted.

Further, the restriction is the least intrusive one which is capable of meeting the required policy outcome. Ensuring that this is so has been achieved in part by providing that the definition of 'cyber-bullying material' that is used in the Online Safety Bill is the narrowest definition available that is consistent with the policy objectives behind the Bill. To be actionable, material must be more than merely offensive or insulting. Importantly, for material to constitute cyber-bullying material under the Online Safety Bill, it must be such that a reasonable person would conclude that it is likely that the material was intended to have an effect on a particular Australian child, and in addition, it must be such that a reasonable person would conclude that the material would be likely to have the effect of seriously threatening, seriously intimidating, seriously harassing or seriously humiliating the Australian child at whom the material is directed.

In addition, there is scope to narrow the notion of 'cyber-bulling material' that can be actioned under the Online Safety Bill further by making legislative rules for the purposes of paragraph 5(1)(d) of the Online Safety Bill. The definition is further narrowed by subclause 5(4) of the Online Safety Bill. This subclause has the effect that material is taken not to be cyber-bullying material if the end-user who posted it was in a position of authority over the child, and posted the material in the lawful exercise of that authority, so long as the posting of the material is reasonable action taken in a reasonable manner.

Having regard to these factors, although the Online Safety Bill restricts the right to freedom of expression of a person who wishes to provide cyber-bullying material on various electronic forums, it does this in the least restrictive manner that is consistent with achieving the intended policy outcome.

The right to freedom of expression is further protected under the Online Safety Bill in that decisions regarding the taking down of cyber-bulling material, which are adverse to an end-user's interests, can be appealed to the Administrative Appeals Tribunal, and reviewed by that Tribunal on their merits.

Protection from unlawful attacks on honour and reputation

Paragraph 1 of Article 16 of the CROC recognises, among other things, the right of a child not to be subjected to unlawful attacks on his or her honour and reputation. Paragraph 2 recognises that children have the right to the protection of the law against such interference or attacks.

Depending on its particular content, cyber-bullying material could constitute interference with a child's privacy, family, home or correspondence or attacks on the child's honour and reputation. By providing a remedy for a child who is the target of cyber-bullying material, hence providing protection of the law against such interferences or attacks, the Online Safety Bill advances the right recognised by Article 16 of the CROC.

Privacy

Paragraph 1 of Article 17 of the ICCPR recognises the right to protection against arbitrary or unlawful interference with privacy, family, home or correspondence. Paragraph 2 of Article 17 of the ICCPR recognises the right of everyone to the protection of the law against such interference.

Paragraph 1 of Article 16 of the CROC recognises, among other things, the right of a child not to be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence. Paragraph 2 recognises that children have the right to the protection of the law against such interference or attacks.

Similar rights are recognised in Article 22 of the CRPD.

The Online Safety Bill engages this right to privacy. Part 9 of the Online Safety Bill deals with disclosure of information that was obtained by the Commissioner as a result of the performance of a function, or the exercise of a power, conferred on the Commissioner by or under the Online Services Bill or the *Broadcasting Services Act 1992* as amended by the Consequential Amendments Bill. The sort of information dealt with by this Part can include information that relates to the child who was the target of the cyber-bullying material, information that relates to the end-user who posted the material, or to other persons.

The Online Safety Bill expressly authorises by law the disclosures that are permitted by Part 9. Further, the Online Safety Bill only authorises disclosures in the particular instances dealt with expressly in Part 9. Each of the instances in which disclosure is authorised would, because of the nature of the authorizing provisions, be reasonable in the circumstances, as discussed below. Accordingly, the Online Safety Bill is consistent with the right against arbitrary interferences with privacy.

The Commissioner will be an 'agency' for the purposes of the *Privacy Act 1988* (the Privacy Act), and hence will be bound by the Privacy Act. Similarly, any body corporate to which the Commissioner delegated functions or powers under clause 64 of the Online Safety Bill would also be bound by the Privacy Act.

Clauses 77 and 78 of the Online Safety Bill authorise disclosure of information by the Commissioner to the Minister responsible for administration of the Online Safety Bill, and also to the Secretary of the Department and APS employees in the Department who are authorised by the Secretary, for the purpose of advising the Minister. Disclosure of information to the Minister, the Secretary and APS employees under these provisions is not arbitrary, as it is a necessary aspect of the constitutional principle of responsible government. In addition, these provisions authorise disclosures to persons who are similarly bound by the Privacy Act.

Clause 79 of the Online Safety Bill authorises the Commissioner to disclose information to a Royal Commission (within the meaning of the *Royal Commissions Act 1902*). Royal Commissions are considered to be the highest form of inquiry into substantive matters of public importance, and it is important that the Commissioner not be prevented from participating in any Royal Commission that is relevant to the Commissioner's area of responsibility. However, to ensure that the right to privacy is protected to the extent possible consistent with the functions and powers of the Royal Commission, subclause 79(2) empowers the Commissioner, by writing, to impose conditions to be complied with in relation to information disclosed under this clause.

Clause 80 of the Online Safety Bill authorises the Commissioner to disclose information to any of a variety of authorities listed in that clause, if the Commissioner is satisfied that the information will enable or assist the authority to perform or exercise any of its functions or powers. The Commissioner is not the only Commonwealth entity with responsibility for children or for matters relating to cyber-bullying, and others, such as the National Children's Commissioner, will have overlapping areas of responsibility. Further, the Online Safety Bill is intended to operate alongside a range of State and Territory laws that deal with various aspects of cyber-bullying (clause 101 of the Online Safety Bill) and is intended not to affect the performance of any State or Territory functions (clause 102 of the Online Safety Bill). In addition, under the Online Safety Bill, the Commissioner is able to refer matters to State or Territory law enforcement agencies (clause 92 of the Online Safety Bill). Because of this, clause 80 of the Online Safety Bill is needed in order to ensure that the Commissioner is able to disclose sufficient information to the authorities listed in that clause to ensure that each of these authorities is able to function to its maximum extent to ensure that the best interests of affected children are protected. To ensure adequate protection of privacy, clause 80 contains a provision similar to subclause 79(2), which empowers the Commissioner, by writing, to impose conditions to be complied with in relation to information disclosed under this clause. This may include, for example, conditions that prevent further disclosure to third parties.

Clauses 81 and 82 are similar provisions, which provide that the Commissioner is able to disclose information to a teacher or school principal, or to a parent or guardian, if the Commissioner is satisfied that the information will assist in the resolution of a complaint under the Online Safety Bill. Resolution of a complaint by teachers or principals, or parents or guardians, has advantages over resolution through the more formal regulatory channels available under the Online Safety Bill, particularly in the case of instances of cyber-bullying that might be of a less serious nature. These clauses facilitate resolution of complaints in such a manner. By facilitating resolution of complaints outside of the more formal channels, the Online Safety Bill is also intending to minimise the adverse impacts of its provisions on the right to freedom of expression, discussed above. Clauses 81 and 82 contain provisions similar to

subclause 79(2), which empower the Commissioner, by writing, to impose conditions to be complied with in relation to information disclosed under these clauses.

Other provisions of Part 9 of the Online Safety Bill are consistent with the right to privacy. Clause 83 permits disclosure of information relating to the affairs of a person, so long as that person has consented to that disclosure, and clause 84 authorises the disclosure of information that is already publicly available. Clause 85 authorises the disclosure of summaries and statistics, but these are only authorised if they are summaries of, or statistics prepared from, 'de-identified' information. The term 'de-identified' is defined in clause 4 as information that is no longer about an identifiable individual, or an individual who is reasonably identifiable. This ensures that the right to privacy is preserved when information is disclosed under this provision.

Minimum guarantees in criminal proceedings

Article 14 of the ICCPR recognises certain minimum guarantees in criminal proceedings such as the presumption of innocence, and fair trial and hearing rights. A penalty may be 'criminal' for the purposes of the ICCPR even if it is 'civil' under Australian domestic law.

Similar rights are recognised in Article 40 of the CROC and Article 13 of the CRPD.

Clause 36 of the Online Safety Bill sets out a civil penalty notice in relation to non-compliance with a social media service notice by a tier 2 social media service. It is therefore necessary to consider whether this amounts to a 'criminal' penalty for the purposes of the ICCPR.

The new civil penalty provision is directed at regulating large social media services, which in almost all instances will be corporations or other organisational bodies, rather than individuals. Accordingly, in general, the new civil penalty provisions will not engage any of the human rights listed above. To the extent that it is theoretically possible than an individual may provide a tier 2 social media service, within the meaning of the Online Safety Bill, it is nevertheless unlikely that the civil penalty notice would be characterised as a 'criminal' penalty for the purposes of the ICCPR, given that the provision is tightly directed at regulating members of a specific group (rather than the public). An application may be made to the Administrative Appeals Tribunal for review of a decision by the Commissioner to issue a social media service notice.

Conclusion

These bills are compatible with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011*. To the extent to which they may engage the right to freedom of expression, the right to protection from unlawful attacks on honour and reputation, the right to privacy and the right to certain minimum guarantees in criminal proceedings, any limitation is reasonable, necessary and proportionate to the goal of enhancing online safety for children.

REGULATION IMPACT STATEMENT

Contents

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]

[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

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.

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]

---

[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

[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

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.

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

---

[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

[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

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

---

[17] www.communications.gov.au/publications/cyber-bullying

[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

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.

---

[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] http://www.communications.gov.au/publications/publications/cyber-bullying

[27] http://www.communications.gov.au/__data/assets/pdf_file/0005/242537/Cyberbullying_Research_Report_-_Part_B.pdf

[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

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]

- 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.

---

[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

[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

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.

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 (eg 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 (eg 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

---

[32] http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11287621
[33] *The Coalition's Policy to Enhance Online Safety for Children*, September 2013

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 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.

---

[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

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 at:
http://www.communications.gov.au/__data/assets/pdf_file/0011/204050/Online-Safety-Consultative-Working-Group-Member-List-FINAL.pdf

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.

8.2 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.

8.3 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]
- Microsoft allows users to report abuse[46]

---

[35] http://info.yahoo.com/legal/au/yahoo/utos/en-au/
[36] https://www.facebook.com/legal/terms
[37] http://www.microsoft.com/info/au-en/cpyright.mspx
[38] https://twitter.com/tos
[39] http://www.google.com.au/intl/en/policies/terms/regional.html
[40] https://www.facebook.com/communitystandards
[41] http://www.youtube.com/t/community_guidelines
[42] http://www.twitter.com/rules
[43] https://www.facebook.com/help/reportlinks
[44] https://support.twitter.com/forms/abusiveuser
[45] http://support.google.com/youtube/bin/answer.py?hl=en&answer=118747
[46] https://support.microsoft.com/contactus/emailcontact.aspx?scid=sw;en;1671&ws=reportabuse

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]

---

[47] http://www.communications.gov.au/__data/assets/pdf_file/0011/220223/Australian_Interactive_Media_Industry_Association.pdf
[48] https://www.facebook.com/notes/facebook-safety/details-on-socialreporting/196124227075034 and https://www.facebook.com/notes/facebook-safety/improvedtools-to-support-your-facebook-experience/473126442708143
[49] http://www.microsoft.com/security/family-safety/default.aspx#Overview.
[50] https://au.safely.yahoo.com/yahoo-products/
[51] https://au.safely.yahoo.com/faq/
[52] http://au.safely.yahoo.com
[53] http://www.google.com.au/goodtoknow/
[54] http://www.google.com.au/safetycenter/
[55] http://pages.ebay.com.au/help/policies/overview.html
[56] http://pages.ebay.com.au/help/account/protecting.html

- 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.

---

[57] http://pages.ebay.com.au/help/policies/tns-tutorials.html
[58] http://support.google.com/youtube/bin/request.py?contact_type=abuse
[59] http://www.facebook.com/safety/groups/parents/
[60] http://www.facebook.com/safety/groups/teachers/
[61] http://www.facebook.com/safety/groups/teens/
[62] https://support.twitter.com/groups/57-safety-security
[63] www.microsoft.com/safety
[64] http://www.microsoft.com/security/family-safety/default.aspx#Products
[65] https://www.facebook.com/beboldstopbullyingau
[66] http://www.amf.org.au/Assets/Files/MEDIA%20RELEASE%20-%20Good%20to%20Know%20Campaign%20helping%20Australians%20stay%20safe%20online.pdf
[67] http://www.canberra.edu.au/cis/tour/
[68] http://cybersmart.gov.au/cybersmart-citizens/~/media/Cybersmart/Digital%20Citizens/Keeping%20Australians%20Safe%20Online%20Public%20Spreads%20July%202014.pdf

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.

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.

[69] http://www.communications.gov.au/__data/assets/pdf_file/0019/161083/Yahoo!.pdf
[70] http://www.communications.gov.au/__data/assets/pdf_file/0004/161077/Facebook.pdf
[71] http://www.communications.gov.au/__data/assets/pdf_file/0017/161081/Microsoft.pdf
[72] http://www.communications.gov.au/__data/assets/pdf_file/0006/161079/Google_YouTube.pdf

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] http://www.afp.gov.au/jobs/current-vacancies/high-tech-crime-operations.aspx
[74] www.education.vic.gov.au/school/principals/health/pages/lol.aspx
[75] http://education.qld.gov.au/studentservices/behaviour/qsaav/cybersafety.html
[76] www.qld.gov.au/education/schools/health/cybersafety/

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] http://det.wa.edu.au/studentsupport/behaviourandwellbeing/detcms/navigation/safe-and-supportive-schools/cyber-safety-websites/?oid=Category-id-13788524
[78] www.digitalcitizenship.nsw.edu.au/index.htm
[79] www.schoolatoz.nsw.edu.au/zh/technology
[80] www.decd.sa.gov.au/speced2/pages/cybersafety/36219/?reFlag=1
[81] www.parentlink.act.gov.au/parenting-resources/parenting-guides/adult-issues/cyber-safety
[82] www.education.nt.gov.au/teachers-educators/students-learning/safe-schools-nt/cybersafety

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

[83] http://www.communications.gov.au/__data/assets/pdf_file/0018/242532/Cyberbullying_Research_Report_-_Part_C.pdf

Providers following public consultation on online social networking by the European Commission (European Social Networking Task Force, 2009).

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.

What are the policy options?

Two policy options are discussed below, including:

---

[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

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.

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.		

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

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

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

[86] http://www.communications.gov.au/publications/publications/cyber-bullying

nature to be considered by police would address a critical gap in existing ways of addressing cyber-bullying.

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:

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.

a. 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.

b. 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.

c. 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.

d. 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] http://www.communications.gov.au/publications/publications/cyber-bullying

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.

ABBREVIATIONS

The following abbreviations are used in this explanatory memorandum:

ACMA	Australian Communications and Media Authority
ACMA Act	*Australian Communications and Media Authority Act 2005*
BSA	*Broadcasting Services Act 1992*
Commissioner	Children's e-Safety Commissioner
Consequential Amendments Bill	Enhancing Online Safety for Children (Consequential Amendments) Bill 2014
Criminal Code	*Criminal Code Act 1995*
FCC	Federal Circuit Court of Australia
FOI Act	*Freedom of Information Act 1982*
Online Safety Bill	Enhancing Online Safety for Children Bill 2014
Regulatory Powers Act	*Regulatory Powers (Standard Provisions) Act 2014*
Special Account	Children's Online Safety Special Account
Telecommunications Act	*Telecommunications Act 1997*
Telecommunications Deregulation Act	*Telecommunications Legislation Amendment (Deregulation) Act 2014*

NOTES ON CLAUSES

ENHANCING ONLINE SAFETY FOR CHILDREN BILL 2014

Part 1—Preliminary

Part 1 of the Online Safety Bill deals with preliminary matters.

Clause 1 – Short title

Clause 1 provides that the Online Safety Bill, when enacted, may be cited as the *Enhancing Online Safety for Children Act 2014*.

Clause 2 – Commencement

Clause 2 provides for the commencement of the Online Safety Bill.

Clauses 1 and 2 of the Online Safety Bill, and anything else not covered in the table at subclause (1), will commence on the day of Royal Assent. Clauses 3 to 108 will commence on a single day to be fixed by Proclamation. However, if the provisions do not commence within the period of 6 months beginning on the day of Royal Assent, they commence on the day after the end of that period.

Clause 3 – Simplified outline of this Act

Clause 3 is a simplified outline of the Online Safety Bill. This simplified outline is included to assist readers to understand the substantive provisions of the Online Safety Bill. However, the outline is not intended to be comprehensive. It is intended that readers should rely on the substantive provisions of the Online Safety Bill.

Clause 4– Definitions

Clause 4 sets out definitions of terms and expressions that are used in the Online Safety Bill. Definitions of particular note include:

- *basic online safety requirements* (see clause 21)
- *cyber-bullying material targeted at an Australian child* (see clause 5 below)
- *relevant electronic service*, which means any of the electronic services listed in the definition including an electronic service that enables end-users to communicate with other end-users by email, instant messaging, short message service (SMS), multimedia message service (MMS), or a chat service or a service that enables end-users to play online games. The definition also includes any electronic service that is specified in legislative rules made by the Minister. The definition of relevant electronic service is relevant to the Commissioner's power to give an end-user notice under Part 5 in relation to material provided on a social media service or a relevant electronic service
- *social media service* (see clause 9)
- *social media service notice*, which means a notice given by the Commissioner to the provider of a social media service under subclause 35(1) requiring the provider to remove certain material from the service.

Other definitional and interpretive provisions are contained in clauses 5, 6, 7, 8, 9, 21, 105 and 106.

Clause 5 – Cyber-bullying material targeted at an Australian child

This clause sets out the criteria for determining whether material submitted as part of a complaint to the Commissioner under clause 18 is 'cyber-bullying material targeted at an Australian child'. This test is also used to determine when the Commissioner may:

- request the provider of a tier 1 social media service to remove material from the service (clause 29);
- give a social media service notice to the provider of a tier 2 social media service (clause 35); or
- give an end-user notice to an end-user of a social media service or relevant electronic service (clause 42).

Subclause (1) applies an objective test in paragraph (b) to determine whether an ordinary reasonable person would conclude that it is likely that the material was intended to have an effect on a particular Australian child, and that the material would be likely to have the effect on the Australian child of seriously threatening, seriously intimidating, seriously harassing or seriously humiliating the Australian child. For the purposes of subclause (1), 'threatening', 'intimidating', 'harassing' and 'humiliating' are intended to have their ordinary meaning.

If all the conditions in paragraphs (a) to (c) are satisfied, then subclause (1) provides that the material in question is 'cyber-bullying material targeted at the Australian child' and the Australian child is the target of the material. The requirement that the material 'was intended to have an effect on the Australian child' in subparagraph (b)(i), is designed to exclude material of a general nature, such as material targeted at a broad class of people.

Paragraph (c) enables other conditions to be included in the test of 'cyber-bullying material targeted at an Australian child' by the legislative rules (see clause 108) should it become apparent during the course of administering the legislation, that further conditions should be specified.

Subclause (2) provides that an effect mentioned in subclause (1) may be a direct result of material being accessed by, or delivered to, the Australian child or an indirect result of the material being access by, or delivered to, one or more other persons. This subclause is intended to capture indirect effects of cyber-bullying material which are not directly accessed by the Australian child, but which still have an effect on the child, for example, by material being accessed by, or delivered to, other children in the child's class at school.

Subclause (3) limits the effect of subclause (1) to the extent that subclause (4) applies.

Subclause (4) provides an exception to subclause (1) for material posted by persons who are in a position of authority over an Australian child, so as not to interfere with reasonable action taken in a reasonable manner by authority figures. Reasonable action taken in a reasonable manner by authority figures such as parents, teachers and employers could include matters such as notifying the child by email of exam results or dismissal from employment. Such matters should not be treated as cyber-bullying.

Clause 6 – When material is provided on a social media service or relevant electronic service

Clause 6 stipulates that material is taken to be 'provided' on a social media service or relevant electronic service if the material is accessible to, or delivered to, one or more of the end-users using the service.

Clause 7 – When material is posted by an end-user of a social media service or relevant electronic service

Clause 7 stipulates that material is taken to be 'posted' on a social media service or relevant electronic service by an end-user if the end-user causes the material to be accessible to, or delivered to, one or more other end-users using the service.

Clause 8 – When material is removed from a social media service or relevant electronic service

Clause 8 stipulates that material is 'removed' from a social media service or relevant electronic service if the material is neither accessible to, nor delivered to, any of the end-users in Australia using the service.

For this purpose, it is intended that if specifically identified material is removed, the material is taken to be removed even if a copy of the same material, within the control of another end-user, is accessible to, or delivered to, one or more other end-users using the service. It would not be reasonable to expect social media services to remove material that is not specifically identified to them.

Clause 9 – Social media service

Clause 9 defines the term 'social media service' for the purposes of the Online Safety Bill.

Subclause (1) provides that a 'social media service' is an electronic service that satisfies the conditions listed in paragraph (a), or is specified in the legislative rules, but does not include an exempt service as defined by subclause (4) or (5).

The term 'electronic service' is defined in clause 4 of the Online Safety Bill as a service that allows end-users to access material using a carriage service or a service that delivers material by means of a carriage service. 'Carriage service' is defined in the Telecommunications Act to mean a service for carrying communications by means of guided or unguided electromagnetic energy. The definition of electronic service specifically excludes broadcasting and datacasting services as defined in the BSA.

Subparagraph 9(1)(a)(i) provides that to be a social media service, the sole or primary purpose of the service must be to enable online social interaction between 2 or more end-users. Subclause 9(1) includes a note making it clear that online social interaction does not include, for example, online business interaction. For example, it is not intended that subparagraph (a)(i) would capture online feedback facilities established by businesses for the purposes of dealing with their customers. Neither is it intended that subparagraph (a)(i) would capture online games that have chat functionality (where the primary purpose of such a service would be to play the game).

Subparagraphs (1)(a)(ii), (iii) and (iv) provide that to be a social media service, the electronic service must allow end-users to link to, or interact with, some or all of the

other end-users, allow end-users to post material on the service and satisfy such other conditions as are set out in legislative rules.

Subclause (2) clarifies that, in the 'sole or primary purpose of the service' test in subparagraph (1)(a)(i), online social interaction includes online interaction that enables end-users to share material for social purposes (which do not include business purposes as clarified by the note).

Subclause (3) clarifies that, in determining whether the 'sole or primary purpose of the service' test in subparagraph (1)(a)(i) is satisfied, the following purposes are to be disregarded:

- the provision of advertising material on the service;
- the generation of revenue from the provision of advertising material on the service.

Subclause (3) will ensure that services that would otherwise meet at least one of the sets of conditions in subclause (1) do not fall outside of the 'social media service' definition on the basis of an argument that the sole or primary purpose of such a service is to sell advertising or generate revenue from advertising sales.

Exempt services

Subclause (4) and (5) provide for exempt services.

A service will be exempt from being a 'social media service' for the purposes of the Online Safety Bill if:

- none of the material on the service is accessible to, or delivered to, one or more end-users in Australia (paragraph (4)(a));
- the service is specified in the legislative rules (paragraph (4)(b)); or
- the Commissioner has made a written declaration that an electronic service is an exempt service for the purposes of clause 9 on the basis of being satisfied that:
  - the service has controls on (i) who can access, or who can be delivered, material provided on the service, or (ii) the material that can be posted on the service; and
  - those controls will be effective in achieving the result that none of the material provided on the service could be cyber-bullying material targeted at an Australian child (subclause (5)).

Subclause (6) provides that an instrument made under subclause (5), by which the Commissioner can declare a particular social media service to be an 'exempt service', is not a legislative instrument. Subclause (6) is declaratory of the law and is included to assist readers rather than create an exception to the *Legislative Instruments Act 2003*.

Clause 10 – Crown to be bound

Clause 10 provides that the Online Safety Bill binds the Crown in each of its capacities, displacing the common law presumption that the Crown is not bound by statutes.

Clause 11 – Application of this Act

Subclause 11(1) provides that the Online Safety Bill extends to every external Territory. The term 'external Territory' is defined in the *Acts Interpretation Act 1901*.

Subclause 11(2) provides that the Online Safety Bill extends to acts, omissions, matters and things outside Australia. The term 'Australia' is defined in clause 4. This provision displaces the common law presumption that statutes do not apply extraterritorially.

Clause 12 – Convention on the Rights of the Child

Clause 12 provides that the Commissioner must, as appropriate, have regard to the Convention on the Rights of the Child in the performance of functions (see clause 15) conferred by or under the Online Safety Bill. Subclause (2) confirms that subclause (1) does not limit the matters to which the Commissioner may have regard.

Part 2—Children's e-Safety Commissioner

Part 2 of the Online Safety Bill deals with the establishment of the Commissioner and sets out the Commissioner's powers and functions. Part 7 of the Online Safety Bill deals with administrative provisions relating to the Commissioner.

Clause 13 – Simplified outline of this Part

Clause 13 is a simplified outline of Part 2 of the Online Safety Bill. This simplified outline is included to assist readers to understand the substantive provisions of Part 2. However, the outline is not intended to be comprehensive. It is intended that readers should rely on the substantive provisions of Part 2.

Clause 14 – Children's e-Safety Commissioner

Clause 14 establishes the statutory office of the Children's e-Safety Commissioner. The note to clause 14 indicates that, in the Online Safety Bill, 'Commissioner' refers to the Children's e-Safety Commissioner, which is a term defined in clause 4 of the Online Safety Bill. The same abbreviation is used in this explanatory memorandum.

Clause 15 – Functions of the Commissioner

Subclause 15(1) sets out the functions of the Commissioner.

Key functions include:

- the functions conferred by the Online Safety Bill, Schedules 5 and 7 to the BSA, or any other Commonwealth law (paragraph (a))
- to promote online safety for children (paragraph (b));
- to coordinate activities of Commonwealth Departments, authorities and agencies relating to online safety for children (paragraph (d));
- to disseminate information relating to online safety for children (paragraph (e));
- to support, conduct and evaluate educational and community awareness programs relevant to online safety for children (paragraph (f));
- to make grants of financial assistance relating to online safety for children (paragraph (g));

- to conduct research about online safety for children (paragraph (h));
- to give the Minister reports and advise about online safety for children (paragraphs (j) and (k));
- to formulate and promote best practice guidelines and statements for persons and bodies involved in online safety for children (paragraphs (p) and (q)).

Subclauses (2) to (4) relate to grants of financial assistance in relation to online safety for children that the Commissioner may make on behalf of the Commonwealth under paragraph (1)(g). The terms and conditions on which financial assistance is granted under paragraph (1)(g) are to be set out in a written agreement between the Commonwealth and the grant recipient.

Subclause (5) clarifies that guidelines and statements formulated under paragraph (1)(p) are not legislative instruments. Subclause (5) is declaratory of the law and is included to assist readers rather than create an exception to the *Legislative Instruments Act 2003*.

In performing his or her functions under clause 15, the Commissioner will be expected to balance the rights and responsibilities of all stakeholders with the need to take proportionate and appropriate action in the best interests of children.

Clause 16 – Powers of the Commissioner

Clause 16 provides that the Commissioner has the power to do all things necessary or convenient to be done for or in connection with the performance of his or her functions. Supplementary powers of the Commissioner with respect to entering into contracts, holding property and receiving money are set out at clause 60.

Part 3—Complaints about cyber-bullying material

Part 3 of the Online Safety Bill provides for a complaints system for cyber-bullying material targeted at an Australian child.

Clause 17 – Simplified outline of this Part

Clause 17 is a simplified outline of Part 3 of the Online Safety Bill. This simplified outline is included to assist readers to understand the substantive provisions of Part 3. However, the outline is not intended to be comprehensive. It is intended that readers should rely on the substantive provisions of Part 3.

Clause 18 – Complaints about cyber-bullying material

Clause 18 of the Online Safety Bill sets out who can make a complaint about cyber-bullying material and the grounds on which a complaint may be made. 'Cyber-bullying material targeted at an Australian child', 'social media service', 'provided' and 'relevant electronic service' are defined terms for the purposes of the Online Safety Bill (see clause 4).

Subclause (1) provides that an Australian child may make a complaint to the Commissioner if the child has reason to believe that he or she was or is the target of cyber-bullying material that has been, or is being, provided on a particular social media service or relevant electronic service.

Subclause (2) enables a 'responsible person' to make a complaint to the Commissioner on behalf of an Australian child if the person has reason to believe that cyber-bullying material targeted at an Australian child has been, or is being, provided on a particular social media service or relevant electronic service. For the purposes of subclause (2), a 'responsible person' is a parent or guardian of the child or a person who the child has authorised to make a complaint on his or her behalf.

There may be circumstances under subclause (2) where a parent or guardian makes a complaint to the Commissioner against the wishes of the child. In such cases, it would be expected that the Commissioner would consider the child's views, consistent with the child's age and maturity, in deciding whether or not to exercise his or her discretion to investigate the complaint under clause 19.

Subclause (3) provides an extension of time for an adult who was an Australian child to make a complaint to the Commissioner, provided that the complaint is made within a reasonable time after the person became aware of the matter and the complaint is made within 6 months after the person reached 18 years. Such a person may make a complaint to the Commissioner if the person has reason to believe that, when he or she was an Australian child, he or she was the target of cyber-bullying material that was provided on a particular social media service or relevant electronic service.

Evidence requirements – complaints about material provided on social media services

If a complaint made by a person to the Commissioner under clause 18 concerns material that has been, or is being, provided on:

- a tier 1 social media service (see Division 2 of Part 4 of the Online Safety Bill) and the person wants the Commissioner to give the provider of the service a notice under clause 29 requesting the provider to remove the material from the service; or
- a tier 2 social media service (see Division 3 of Part 4 of the Online Safety Bill) and the person wants the Commissioner to give the provider of the service a social media service notice under clause 35 requiring the provider to remove the material from the service;

the complaint made under clause 18 must be accompanied by evidence that the material was the subject of a complaint that was previously made under the service's complaint scheme (see subclause (4) and (5)).

Subclause (6) provides that, for the purposes of subclauses (4) and (5), evidence must be in a form required by the Commissioner. Subclauses (7) and (8) provide that the Commissioner may require evidence to be in the form of a receipt, complaint number, screen shot, statutory declaration, or another specified form in certain circumstances. However, subclauses (7) and (8) do not limit subclause (6) (see subclause (9)). Subclause (10) provides that a requirement under subclauses (6), (7) or (8) is not a legislative instrument. Subclause (10) is declaratory of the law and is included to assist readers rather than create an exception to the *Legislative Instruments Act 2003*.

Clause 19 – Investigation of complaints

Subclause 19(1) provides that the Commissioner may investigate a complaint made under clause 18. The Commissioner is not required to investigate all complaints made under clause 18 and may use his or her discretion in deciding whether or not to investigate any particular complaint.

In some cases, the Commissioner might decline to investigate a complaint under clause 18, and instead refer the matter to a law enforcement agency in accordance with clause 92, if the Commissioner is satisfied that the material is of a sufficiently serious nature to warrant referral to a law enforcement agency in accordance with that clause.

A decision not to investigate a complaint is not reviewable under the Online Safety Bill (clause 88 deals with review of decisions under the Online Safety Bill). Instead, review of such a decision would be governed by the *Administrative Decisions (Judicial Review) Act 1977* and section 39B of the *Judiciary Act 1903*.

The Commissioner may choose to not investigate certain other types of complaints, for example, complaints which are frivolous or vexatious or complaints which may be best resolved by the relevant school.

Subclauses 19(2) and (3) provide that an investigation under this clause is to be conducted as the Commissioner thinks fit, and that the Commissioner may, for the purposes of an investigation, obtain information from such persons, and make such inquiries, as he or she thinks fit. It is expected that the Commissioner will develop appropriate procedures for the acceptance, investigation and closing of complaints.

Subclause (4) provides that subclauses (1) to (3) have effect subject to Part 13 of the BSA (Part 13 of the BSA, as proposed to be amended by the Consequential Amendments Bill, confers certain investigative powers on the Commissioner).

Subclause (5) provides that the Commissioner may terminate an investigation made under clause 19. For example, the Commissioner might decide to terminate an investigation where the matter is of a criminal nature and would be better dealt with by police.

Part 4—Social media services

Part 4 of the Online Safety Bill deals with the treatment of cyber-bullying material on social media services.

Division 1—Introduction

Division 1 of Part 4 of the Online Safety Bill deals with introductory material relating to Part 4, including basic online safety requirements and Parliament's expectations.

Clause 20 – Simplified outline of this Part

Clause 20 is a simplified outline of Part 4 of the Online Safety Bill. This simplified outline is included to assist readers to understand the substantive provisions of Division 1 of Part 4. However, the outline is not intended to be comprehensive. It is intended that readers should rely on the substantive provisions of Part 4.

Clause 21 – Basic online safety requirements

Clause 21 outlines the basic online safety requirements which apply to social media services and are referred to in the statement of Parliamentary expectations set out in clause 22 below. Subclause 21(2) notes that *cyber-bullying material* has its ordinary meaning for the purposes of clause 21.

To meet the basic online safety requirements, a social media service must:

- have terms of use that prohibit end-users from posting cyber-bullying material on the service (clause 104 of the Online Safety Bill clarifies what may be regarded as the equivalent of provisions prohibiting end-users from posting cyber-bullying material on the service) (paragraph 21(1)(a));
- have a complaints scheme under which end-users can request removal of cyber-bullying material (paragraph 21(1)(b)); and
- have a designated contact person for the purposes of the Online Safety Bill (paragraph 21(1)(c)) whose contact details are notified to the Commissioner (paragraph 21(1)(d)).

Compliance with the basic online safety requirements is a prerequisite for the Commissioner to declare a social media service to be a 'tier 1 social media service' under clause 23 and is a factor to which the Commissioner must have regard in deciding whether to make a recommendation under subclause 31(1) that the Minister declare a specified service to be a 'tier 2 social media service'.

If the Commissioner is satisfied that a social media service does not comply with the basic online safety requirements, the Commissioner may publish a statement to that effect under clause 38**.**

Clause 22 – Statement of Parliamentary expectations

Clause 22 outlines Parliament's expectations for social media services and the Commissioner.

Subclause (1) establishes Parliament's expectation that social media services will comply with the basic online safety requirements.

Subclause (2) establishes Parliament's expectation that the Commissioner, as far as practicable, should communicate the expectation in subclause (1) to providers of social media services.

Subclause (3) makes it clear that subclauses (1) and (2) do not impose a duty enforceable in a court.

Division 2—Tier 1 social media services

Division 2 of Part 4 deals with tier 1 social media services.

Subdivision A—Declaration of tier 1 social media service

Subdivision A of Division 2 of Part 4 deals with declarations of tier 1 social media services.

Clause 23 – Declaration of tier 1 social media service

Clause 23 establishes the grounds and processes by which a social media service may apply to the Commissioner for declaration as a tier 1 social media service. The clause also outlines the circumstances in which the Commissioner must declare a social media service to be a tier 1 social media service.

Subclause (1) enables a social media service to apply to the Commissioner for declaration as a tier 1 social media service. Subclause (2) imposes form requirements for an application made under subclause (1). Subclause (3) creates an option for a service making an application under subclause (1) to elect to receive requests for

removal of cyber-bullying material under clause 29 in accordance with the 'special rule' under subclause 29(2) (by which the Commissioner must consider whether material breaches relevant provisions in the service's terms of use), rather than the 'default rule' under subclause 29(1).

Subclause (4) establishes the circumstances in which the Commissioner is required to grant a social media service tier 1 status.

Subclause (5) establishes the circumstances in which the Commissioner must not declare a social media service a tier 1 social media service. In accordance with paragraph (d), the Commissioner must give notice of the refusal to the applicant in writing. An application may be made to the Administrative Appeals Tribunal, by the provider of the social media service concerned, for review of a decision of the Commissioner to refuse to make a declaration in relation to a social media service under subclause 23(5) (subclause 88(1) refers).

Subclause (6) confirms that a declaration made under subclause (4) is not a legislative instrument for the purposes of the Online Safety Bill. Subclause (6) is declaratory of the law and is intended to assist readers.

Clause 24 – Variation of declaration of tier 1 social media service—change of name

Clause 24 allows the Commissioner to vary a declaration made under subclause 23(4) in certain circumstances.

Subclause (1) gives the Commissioner power to vary a declaration by writing where a social media service changes its name.

Subclause (2) requires the Commissioner to notify the provider of the social media service in writing of any such variation.

Subclause (3) confirms that a variation made under subclause (1) is not a legislative instrument. Subclause (3) is declaratory of the law and is intended to assist readers.

Clause 25 – Revocation of declaration of social media service as a tier 1 social media service

Clause 25 allows the Commissioner to revoke a declaration of a tier 1 social media service on specific grounds.

Subclause (1) gives the Commissioner the power to revoke a declaration of a tier 1 social media service, made under clause 23, where at least 12 months have passed since the declaration was made (subparagraph (a)(i)) and where during the preceding 12 months the provider has repeatedly failed to comply with requests for removal of cyber-bullying material under clause 29 (subparagraph (a)(ii)). The word 'repeatedly' in this clause is intended to have its ordinary meaning. The Commissioner may also revoke a declaration of a tier 1 social media service, made under clause 23, where the Commissioner is satisfied that the service does not comply with the basic online safety requirements (paragraph (b)). An application may be made to the Administrative Appeals Tribunal, by the provider of the social media service concerned, for review of a decision of the Commissioner to revoke a declaration under clause 25 (subclause 88(1) refers).

Subclause (2) provides that the Commissioner must give written notice of any revocation made under subclause (1) to the provider of the service.

Subclause (3) restricts a provider of a social media service who has had a declaration of a tier 1 social media service revoked from reapplying for a declaration under clause 23(1), for a period of 28 days after the day the declaration was revoked. This is intended to provide the Commissioner with sufficient time to consider whether to recommend to the Minister that the service be declared under tier 2.

Subclause (4) confirms that a revocation made under clause 25(1) is not a legislative instrument for the purposes of the Online Safety Bill. Subclause (4) is declaratory of the law and is intended to assist readers.

Clause 26 – Notification of changes to terms of use of tier 1 social media service

Clause 26 creates obligations for providers of a tier 1 social media service to notify the Commissioner of changes to its terms of use in certain circumstances. If a change to the terms of use occurs and the change could affect cyber-bullying material, the provider of the service must give the Commissioner written notice of the change within 14 days after the change was made. Notice of the change may be given electronically. Subclause 26(2) states that for the purposes of clause 26, *cyber-bullying material* has its ordinary meaning.

Clause 27 – Notification of change of contact person etc.

Clause 27 creates obligations for providers of tier 1 social media services to notify the Commissioner of any changes to the identity or contact details of the individual designated as the service's contact person. Notice of change must be given to the Commissioner in writing within 14 days after the change occurs. Notice of the change may be given electronically.

Clause 28 – Register of Tier 1 Social Media Services

Clause 28 outlines the Commissioner's obligations to maintain an electronic register of tier 1 social media services, to be made available on the Commissioner's website. Subclause 28(4) clarifies that the register is not a legislative instrument, and is declaratory of the law.

Subdivision B—Request for removal of cyber-bullying material

Clause 29 – Request for removal of cyber-bullying material

Clause 29 sets out the circumstances in which the Commissioner may request a tier 1 social media service provider to remove cyber-bullying material targeted at an Australian child from its service. Clause 29 sets out two rules (the 'default rule' and the 'special rule') which provide options for social media services in being given requests to remove content from services. In considering complaints in accordance with the 'special rule', the Commissioner must consider whether the material requested to be removed from the social media service breaches the cyber-bullying provision in the service's terms of use. The 'default rule' requires the Commissioner to consider the statutory test at clause 5 in determining whether content on the service is cyber-bullying material. Social media service providers may elect, in their application to the Commissioner for declaration as a tier 1 service, to apply the special rule (subclause 23(3) refers), otherwise the default rule will apply.

A written notice provided by the Commissioner under either subclause 29(1) or (2) may request the provider to remove specified material, the subject of the complaint,

from the service within 48 hours. A removal notice does not impose an ongoing obligation for a social media service to keep removed material from the service, if the material is reposted by an end-user. In such instances, a further complaint would need to be made to the service.

Subclause 29(3) relates to circumstances where a social media service provider elects, through a statement covered by subclause 23(3), for the Commissioner to use the 'special rule' in requesting the removal of content. Subclause 29(3) provides that if the service does not have a provision which prohibits the posting of cyber-bullying material, or an equivalent provision, then the subclause 23(3) statement in the provider's application for tier 1 status may be disregarded, with the effect that the 'default rule' would be used by the Commissioner in requesting the removal of content.

For the purposes of paragraphs (2)(b) and (3)(b), subclause (4) clarifies that *cyber-bullying material* has its ordinary meaning.

Division 3—Tier 2 social media services

Division 3 of Part 4 deals with tier 2 social media services.

Subdivision A—Declaration of tier 2 social media service

Subdivision A of Division 3 of Part 4 deals with declarations of tier 2 social media services.

Clause 30 – Declaration of tier 2 social media service

Clause 30 enables the Minister to declare, by legislative instrument, that a specified social media service is a 'tier 2 social media service' for the purposes of the Online Safety Bill. Subclause (2) prohibits the Minister from declaring a tier 2 social media service unless the Commissioner has made a recommendation under clause 31 that the Minister declare the service.

Clause 31 – Recommendation about declaration of a tier 2 social media service

Clause 31 enables the Commissioner to recommend that the Minister declare a specified social media service to be a tier 2 social media service under subclause 30(1) of the Online Safety Bill. Subclauses 31(2) to (7) specify criteria that the Commissioner must apply before making any recommendation under subclause 31(1).

The Commissioner must not make such a recommendation in relation to a service that is a tier 1 social media service (subclause 31(2)). The Commissioner also must not make such a recommendation to the Minister unless the Commissioner is satisfied the service is a 'large social media service', having regard to factors in subclause 31(8), or the provider of the social media service has requested the Commissioner to make the recommendation.

Furthermore, the Commissioner must also give adequate opportunity, in accordance with subclause (4), for the provider of a social media service which has never had tier 1 status to apply for tier 1 status before making a recommendation to the Minister under subclause (1) with respect to tier 2 status.

Subclause (5) sets out a range of factors which the Commissioner must consider before making a recommendation under subclause 31(1). These factors include:

- whether the service complies with the basic online safety requirements, described at clause 21 above – a failure to comply would strengthen the case for tier 2 declaration;
- whether the provider of the service has failed to make an application under subclause 23(1) for a declaration of the service as tier 1 social media service – a failure to apply for tier1 status when given the opportunity would strengthen the case for tier 2 declaration ;
- whether a subclause 23(4) declaration (as a tier 1 social media service) relating to the service has been revoked under clause 25 – such a revocation would strengthen the case for tier 2 declaration; and
- such other matters (if any) as the Commissioner considers relevant.

In determining whether a social media service is a large social media service, for the purposes of subclause 31(3), the Commissioner must under subclause 31(8) have regard to the number of accounts held by end-users who are (i) ordinarily resident in Australia; and (ii) Australian children. The relevant social media service may not have this information available or may not make it available to the Commissioner. Accordingly, the Commissioner may make reasonable assumptions and estimates (subclause (9)). Under subclause 31(10), the Commissioner may publish a statement on the Commissioner's website explaining the Commissioner's approach to administering subclauses 31(8) and (9).

Subclause 31(11) provides that such a statement is not a legislative instrument. A statement published under subclause 31(10) is not a legislative instrument within the meaning of section 5 of the *Legislative Instruments Act 2003* and so the statement does not represent a substantive exemption from the requirements of that Act.

Clause 32 – Variation of declaration of tier 2 social media service—change of name

Clause 32 allows the Minister, by legislative instrument, to vary a tier 2 declaration in force under subclause 30(1) in circumstances where the service has changed its name.

Clause 33 – Revocation of declaration of social media service as a tier 2 social media service

Clause 33 establishes the circumstances in which the Minister may revoke a subclause 30(1) declaration in relation to a service's status as a tier 2 social media service For example, it is expected that revocation of tier 2 status would likely occur where a provider of a tier 2 service has demonstrated a good record of compliance with social media service notices from the Commissioner under clause 35, and has indicated that it would prefer to work cooperatively under tier 1 of the scheme. The Minister may only revoke a subclause 30(1) declaration where the service complies with the basic online safety requirements set out in clause 21; where at least three months have passed since the declaration was made; where the service has complied with all (or nearly all) social media service notices given within the preceding three months; and where the Commissioner has recommended revocation of the declaration.

Subclause (2) provides that any revocation made under subclause (1) takes effect at the end of the 28-day period which begins at the end of the day that the revocation was made. If the provider of the service made an application during that 28-day

period for declaration as a tier 1 social media service under subclause 23(1), paragraph 23(4)(c) does not apply. Paragraph 23(4)(c) establishes the requirement for a social media service to not be a tier 2 social media service when applying for a tier 1 declaration. This requirement would be inappropriate in the circumstances where a revocation is made, but has not yet taken effect.

The cumulative effect of subclauses (1) to (3) is to ensure the smooth transition of social media services from tier 2, to tier 1 in the specified circumstances.

Clause 34 – Register of Tier 2 Social Media Services

Clause 34 requires the Commissioner to maintain an electronic register of all tier 2 social media services, and to make the register available for inspection on the Commissioner's website. Subclause 34(4) clarifies that the register is not a legislative instrument, and is declaratory of the law.

Subdivision B—Social media service notices

Subdivision B of Division 3 of Part 4 deals with requirements for social media service notices.

Clause 35 – Social media service notice

Clause 35 establishes the grounds on which the Commissioner may give the provider of a tier 2 social media service a social media service notice, requiring the provider to remove the material which is subject of the complaint from the service within 48 hours after the receiving the notice.

The Commissioner may only give a social media service notice where the material has been the subject of a complaint under the service's complaints scheme and the material was not removed within 48 hours (or such longer period as the Commissioner allows), a complaint has been made to the Commissioner under clause 18 and the Commissioner is satisfied that the material is (or was) cyber-bullying material targeted at an Australian child, within the meaning of clause 5.

The Commissioner may refuse to give a social media service notice but in those circumstances must, under subclause 35(2), advise the complainant in writing of the refusal to issue a social media service notice.

An application may be made to the Administrative Appeals Tribunal, by either the provider of the social media service concerned or the end-user who posted the material, for review of a decision of the Commissioner to give a social media service notice under clause 35 (subclauses 88(3)-(4) refer).

An application to the Administrative Appeals Tribunal may also be made, by either a person who made the complaint about cyber-bullying material under clause 18 or by (or with the consent of) the person who was the target of the material, for review of a decision of the Commissioner to refuse to give a social media service notice (subclauses 88(5)-(6) refer).

Clause 36 – Compliance with social media service notice

Clause 36 provides that a person must comply with a requirement under a social media service notice to the extent that they are capable of doing so. Breach of clause 36 is a civil penalty of 100 penalty units ($17,000).

Civil penalty provisions in the Online Safety Bill are enforceable under Part 4 of the Regulatory Powers Act, in accordance with subclause 46(1).

If a provider refuses to comply with a social media service notice, daily penalties for contraventions of clause 36 apply under section 93 of Regulatory Powers Act.

Clause 37 – Formal warning

Clause 37 enables the Commissioner to issue a formal warning if a person contravenes clause 36.

Division 4—Non-compliant social media services

Division 4 of Part 4 allows the Commissioner to prepare and publish written statements where social media services do not comply with the basic online safety requirements under clause 21, a request for removal of cyber-bullying material under clause 29 or a social media service notice under clause 35.

Clause 38 – Non-compliance with the basic online safety requirements

Clause 38 gives the Commissioner the authority to prepare and publish a statement on the Commissioner's website that a social media service does not comply with the basic online safety requirements.

Where a statement has been published under subclause (1), subclause (2) requires the Commissioner to remove that statement from the Commissioner's website when the Commissioner is satisfied that the service does comply with the basic online safety requirements.

Clause 39 – Non-compliance with a request for removal of cyber-bullying material

Clause 39 gives the Commissioner the authority to prepare and publish a statement on the Commissioner's website that a tier 1 social media service has not complied with a request for removal of cyber-bullying material under clause 29.

Clause 40 – Non-compliance with a social media service notice

Clause 40 gives the Commissioner the authority to prepare and publish a statement on the Commissioner's website that a tier 2 social media service has not complied with a social media service notice.

Part 5—End-user notices

Part 5 deals with end-user notices that may be given to a person who posts cyber-bullying material targeted at an Australian child.

Clause 41 – Simplified outline of this Part

Clause 41 is a simplified outline of Part 5 of the Online Safety Bill. This simplified outline is included to assist readers to understand the substantive provisions of Part 5. However, the outline is not intended to be comprehensive. It is intended that readers should rely on the substantive provisions of Part 5.

Clause 42 – End-user notice

Clause 42 enables the Commissioner to give a notice (an end-user notice) to a person who posts cyber-bullying material targeted at an Australian child on a social media service or relevant electronic service.

An end-user notice may require the end-user to take reasonable steps to remove the material within a specified period, to refrain from posting any cyber-bullying material for which the child is the target and/or to apologise to the subject for posting the material (including in a specified manner and within a specified time). By focusing on the end-user who posted the material, a notice under clause 42 is quite different from a social media service notice under clause 35, which is directed at the provider of the social media service.

Subclause (2) is a transitional provision which disapplies paragraph 42(1)(a) in circumstances where the material considered for an end-user notice was posted before the commencement of clause 42 unless it was provided on the service after the commencement of clause 42. This allows material which is posted prior to the enactment of clause 42 to nevertheless be considered by the Commissioner for the purpose of an end-user notice if it remains posted, but prevents the legislation operating retrospectively.

An application may be made to the Administrative Appeals Tribunal for review of a decision of the Commissioner to give an end-user notice under clause 42 (subclause 88(7) refers).

Clause 43 – Compliance with end-user notice

Clause 43 requires a person to comply with a requirement under an end-user notice to the extent that the person is capable of doing so. There may be instances where an end-user is unable to prevent cyber-bullying continuing, such as where content has been further disseminated by other parties. In such circumstances, the end-user can only be held responsible for steps the person is capable of undertaking. Clause 43 is enforceable under Part 7 of the Regulatory Powers Act which creates a framework for using injunctions to enforce provisions (see clause 48).

Clause 44 – Formal warning

Clause 44 allows the Commissioner to issue a formal warning if a person contravenes clause 43. In administering Part 5, the Commissioner can be expected to develop appropriate policies and procedures, such as ‘show cause notices’ to ensure that procedural fairness is afforded to end-users subject to notices in accordance with standard administrative law requirements.

Part 6—Enforcement

Part 6 deals with enforcement provisions under the Online Safety Bill and applies the civil penalty, enforceable undertaking and injunction frameworks in the Regulatory Powers Act to the Online Safety Bill.

Clause 45 – Simplified outline of this Part

Clause 45 is a simplified outline of Part 6 of the Online Safety Bill. This simplified outline is included to assist readers to understand the substantive provisions of Part 6.

However, the outline is not intended to be comprehensive. It is intended that readers should rely on the substantive provisions of Part 6.

Clause 46 – Civil penalty provision

Subclause 46(1) provides for the enforceability of civil penalty provisions in the Online Safety Bill under Part 4 of the Regulatory Powers Act. Compliance with a social media service notice is a civil penalty provision under clause 36 of the Online Safety Bill. The note to subclause (1) provides that Part 4 of the Regulatory Powers Act allows a civil penalty provision to be enforced by obtaining an order for a person to pay a pecuniary penalty for the contravention of the provision.

Subclause (2) provides that, for the purposes of Part 4 of the Regulatory Powers Act, the Commissioner is an authorised applicant in relation to a civil penalty provision in the Online Safety Bill.

Subclause (3) provides that, for the purposes of Part 4 of the Regulatory Powers Act, the Federal Circuit Court of Australia (FCC) is a relevant court in relation to a civil penalty provision in the Online Safety Bill. While the FCC is nominated as a relevant court for the purposes of Part 4 of the Regulatory Powers Act, matters in relation to a civil penalty provision in the Online Safety Bill may be transferred from the FCC to the Federal Court of Australia, where appropriate.

Subclause (4) extends the applicability of Part 4 of the Regulatory Powers Act in relation to a civil penalty provision in the Online Safety Bill to every external Territory and to acts, omissions, matters and things outside Australia.

Clause 47 – Enforceable undertakings

Subclause 47(1) provides that clause 36 of the Online Safety Bill (which is a civil penalty provision in relation to compliance with social media service notices) is enforceable under Part 6 of the Regulatory Powers Act. Part 6 of the Regulatory Powers Act creates a framework for accepting and enforcing undertakings in relation to compliance with provisions.

Subclause (2) provides that, for the purposes of Part 6 of the Regulatory Powers Act, the Commissioner is an authorised person in relation to clause 36 of the Online Safety Bill.

Subclause (3) provides that, for the purposes of Part 6 of the Regulatory Powers Act, the FCC is a relevant court in relation to clause 36 of the Online Safety Bill. While the FCC is nominated as a relevant court in relation to clause 36 of the Online Safety Bill for the purposes of Part 6 of the Regulatory Powers Act, such matters may be transferred from the FCC to the Federal Court of Australia, where appropriate.

Subclause (4) extends the applicability of Part 6 of the Regulatory Powers Act in relation to clause 36 of the Online Safety Bill to every external Territory and to acts, omissions, matters and things outside Australia.

Clause 48 – Injunctions

Subclause 48(1) provides that clauses 36 (compliance with social media service notices) and 43 (compliance with end-user notices) are enforceable under Part 7 of the Regulatory Powers Act. Part 7 of the Regulatory Powers Act creates a framework for using injunctions to enforce provisions.

Subclause (2) provides that, for the purposes of Part 7 of the Regulatory Powers Act, the Commissioner is an authorised person in relation to clauses 36 and 43 of the Online Safety Bill.

Subclause (3) provides that, for the purposes of Part 6 of the Regulatory Powers Act, the FCC is a relevant court in relation to clauses 36 and 43 of the Online Safety Bill. While the FCC is nominated as a relevant court in relation to clauses 36 and 43 of the Online Safety Bill for the purposes of Part 7 of the Regulatory Powers Act, such matters may be transferred from the FCC to the Federal Court of Australia, where appropriate

Subclause (4) extends the applicability of Part 7 of the Regulatory Powers Act in relation to clauses 36 and 43 of the Online Safety Bill to every external Territory and to acts, omissions, matters and things outside Australia.

Part 7—Administrative provisions relating to the Commissioner

Part 7 deals with the administrative provisions relating to the Commissioner, including appointment of the Commissioner, supplementary powers of the Commissioner, obligations of the Commissioner and the ACMA's obligation to assist the Commissioner.

Division 1—Introduction

Division 1 of Part 7 sets out introductory provisions for Part 7.

Clause 49 – Simplified outline of this Part

Clause 49 is a simplified outline of Part 7 of the Online Safety Bill. This simplified outline is included to assist readers to understand the substantive provisions of Part 7. However, the outline is not intended to be comprehensive. It is intended that readers should rely on the substantive provisions of Part 7.

Division 2—Appointment of the Commissioner

Division 2 of Part 7 sets out provisions related to the appointment of the Commissioner.

Clause 50 – Appointment of the Commissioner

Subclause 50(1) provides that the Commissioner is to be appointed by the Minister by written instrument.

Subclause 50(2) sets out the eligibility criteria for appointment as the Commissioner. The Minister must be satisfied that a person has substantial experience or knowledge and significant standing in at least one of the fields listed in paragraphs (c) to (f). These include:

- the operation of social media services;
- the operation of the internet industry;
- public engagement on issues relating to online safety;
- public policy in relation to the communications sector.

Subclause 50(3) provides that the Commissioner holds office on a full-time basis.

Clause 51 – Period of appointment for the Commissioner

Clause 51 provides that the Commissioner holds office for the period specified in the instrument of appointment (see subclause 50(1)). This period must not exceed 5 years. The note to clause 51 indicates that the Commissioner may be reappointed as per the *Acts Interpretation Act 1901*.

Clause 52 – Acting appointments

Subclause 52(1) provides that the Minister may appoint a person to act as the Commissioner when there is a vacancy in the office of the Commissioner, or during any period where the Commissioner is absent from duty or Australia, or is unable to perform the duties of the office.

The note to subclause (1) refers readers to the rules that apply to acting appointments under section 33A of the *Acts Interpretation Act 1901*.

Subclause 52(2) provides that a person can only act as the Commissioner if he or she meets the same eligibility requirements for appointment as the Commissioner (see clause 50).

Division 3—Terms and conditions for the Commissioner

Division 3 provides the terms and conditions for the Commissioner's appointment.

Clause 53 – Remuneration and allowances

Clause 53 sets out conditions in relation to remuneration and allowances applicable to the Commissioner's appointment.

Subclause (1) provides that the Commissioner's remuneration is to be determined by the Remuneration Tribunal. Where no determination by the Remuneration Tribunal is in operation, the Commissioner is to be paid the remuneration that is prescribed by the legislative rules.

Subclause (2) provides that the Commissioner is to be paid allowances prescribed by the legislative rules.

Subclause (3) provides that clause 53 is subject to the *Remuneration Tribunal Act 1973*.

Clause 54 – Leave of absence

Subclause 54(1) provides that the Commissioner has entitlements to recreation leave as determined by the Remuneration Tribunal.

Subclause 54(2) provides that the Minister may grant the Commissioner leave of absence, other than recreational leave, on terms and conditions determined by the Minister.

Clause 55 – Outside employment

Clause 55 prohibits the Commissioner from engaging in paid employment outside the duties of his or her office without the Minister's approval.

Clause 56 – Disclosure of interests to the Minister

Clause 56 set outs the Commissioner's disclosure of interest obligations.

Clause 57 – Resignation

Subclause 57(1) provides that the Commissioner may resign his or her appointment by giving the Minister a written resignation.

Subclause 57(2) provides that the resignation will take effect on the date the Minister receives the written resignation or on a later date specified in the resignation.

Clause 58 – Termination of appointment

Clause 58 provides the grounds on which the Minister may terminate the Commissioner's appointment.

Clause 59 – Other terms and conditions

Clause 59 provides that the Commissioner holds office subject to any further terms and conditions not covered by the Online Safety Bill that are determined by the Minister.

Division 4—Other matters

Clause 60 – Supplementary powers

Clause 60 sets out the supplementary powers of the Commissioner.

The Commissioner's powers include the power to enter into contracts on behalf of the Commonwealth (subclauses (1) and (2)).

Any property held by the Commissioner is held for and on behalf of the Commonwealth (subclause (3)). Any money received by the Commissioner is received for and on behalf of the Commonwealth (subclause (4)).

Subclause (5) prohibits the Commissioner from holding real or personal property, or money, on trust for any person other than the Commonwealth. The note to subclause (5) states that the Commonwealth may hold real or personal property, or money, on trust.

Subclause (6) clarifies that the right to sue is taken not to be personal property for the purposes of subclause (3).

Clause 61 – Commissioner's liabilities are Commonwealth liabilities

Clause 61 provides that any of the Commissioner's financial liabilities are to be taken to be liabilities of the Commonwealth.

Subclause (2) provides a definition of 'financial liability' for the purposes of clause 61.

Clause 62 – Commissioner has privileges and immunities of the Crown

Clause 62 provides that the Commissioner has the privileges and immunities of the Crown in right of the Commonwealth.

Clause 63 – Delegation by the Commissioner to a member of the staff of the ACMA etc.

Subclause 63(1) provides that the Commissioner may, by writing, delegate any or all of the Commissioner's functions and powers to certain members of the staff of the ACMA or persons whose services are made available to the ACMA under paragraph 55(1)(a) of the ACMA Act.

Subclause 63(2) requires a delegate of the Commissioner to comply with any written directions of the Commissioner.

Subclause 63(3) prohibits the Commissioner from delegating the power to make, vary or revoke a legislative instrument.

Clause 64 – Delegation by the Commissioner to a body corporate

Subclause 64(1) provides that the Commissioner may, by writing, delegate any or all of the Commissioner's functions and powers under Part 3 or Part 4 (except clauses 35 or 37) of the Online Safety Bill to a body corporate that meets certain criteria set out at paragraphs (c) to (e).

Subclause 64(2) requires a delegate under this clause to comply with any written directions of the Commissioner.

Subclause 64(3) provides for the exchange of information between a delegated body corporate entity and the Commissioner that is relevant to the performance or exercise of the functions or powers of the Commissioner.

Subclause 64(4) enables the legislative rules to provide that a body corporate to which powers or functions have been delegated in accordance with this clause, is a body corporate established for a public purpose, for the purposes of any specified law of the Commonwealth other than the Online Safety Bill.

Subclause 64(5) provides that the Minister may enter into an agreement with a body corporate, to which the Commissioner has delegated functions or powers, to remunerate the body corporate for performing or exercising those delegated functions, or powers.

Clause 65 – Sub-delegation by body corporate

Subclause 65(1) allows for a body corporate to whom the Commissioner has delegated functions or powers, to sub-delegate those functions or powers to a person who is a director or employee of the body corporate and satisfies the conditions set out in the legislative rules.

Subclause 65(2) requires a sub-delegate to comply with any written directions of the body corporate or the Commissioner.

Subclause 65(3) provides that sections 34AA, 34AB and 34A of the *Acts Interpretation Act 1901* apply to a sub-delegation in a corresponding way to the way that they apply to a delegation.

Clause 66 – Annual report

Subclause 66(1) requires the Commissioner to prepare and give to the Minister, for presentation to the Parliament, an annual report as soon as practicable after the end of each financial year on the operations of the Commissioner during that year. The note

to subclause (1) refers to additional rules about annual reports in section 34C of the *Acts Interpretation Act 1901*.

Subclause 66(2) requires a report made under subclause (1) to include a report on the operations under the Online Safety Bill during the year of a body corporate to which the Commissioner has delegated one or more functions or powers.

Clause 67 – Assistance to the Commissioner

Clause 67 requires the ACMA to assist the Commissioner to perform his or her functions and exercise his or her powers, including by making available members of the staff of the ACMA, and to do so to the extent the Commissioner reasonably requires (subclauses (1) and (3)). Such assistance may include the provision of advice and the making available of resources and facilities (subclause (2)).

Subclause (4) enables the Minister, by legislative instrument, to give directions to the ACMA in relation to the performance or exercise of its functions or powers under clause 67. The notes to subclause (4) refer to the power to vary and revoke instruments under subsection 33(3) of the *Acts Interpretation Act 1901* and sections 44 and 54 of the *Legislative Instruments Act 2003* which provide that the disallowance and sunsetting arrangements under that Act do not apply to Ministerial directions.

The ACMA must comply with a direction made under subclause (4) (subclause (5)).

Subclause (6) provides that, for the purpose of clause 67, a member of the staff of the ACMA includes an officer or employee whose services are made available to the ACMA under paragraph 55(1)(a) of the ACMA Act.

Clause 68 – Commissioner not subject to direction by the ACMA

Clause 68 clarifies that the Commissioner is not subject to direction by the ACMA, any of its members or associate members, or any member of its staff in relation to the performance of a function, or the exercise of a power, by the Commissioner.

Clause 69 – Consultants

Subclause 69(1) enables the Commissioner, on behalf of the Commonwealth, to engage consultants that have suitable qualifications and experience. Consultants are to be engaged on the terms and conditions that the Commissioner determines in writing (subclause 69(2)).

Clause 70 – Minister may give directions to the Commissioner

Subclause 70(1) enables the Minister, by legislative instrument, to give directions to the Commissioner about the performance of the Commissioner's functions or exercise of the Commissioner's powers. The notes to subclause (1) refer to the power to vary and revoke instruments under subsection 33(3) of the *Acts Interpretation Act 1901* and sections 44 and 54 of the *Legislative Instruments Act 2003* which provide that the disallowance and sunsetting arrangements under that Act do not apply to Ministerial directions.

Subclause 70(2) provides that directions made under subclause (1) must be of a general nature only.

Subclause 70(3) provides that subclause (2) does not apply to the Commissioner's powers under subclause 64(1) (which deals with delegation to a body corporate).

The Commissioner is required to comply with a direction made under subclause (1) (subclause 70(4)).

Part 8—Children's Online Safety Special Account

Part 8 establishes the Children's Online Safety Special Account (Special Account) and provides for how moneys may be credited to or debited from the Special Account.

Clause 71 – Simplified outline of this Part

Clause 71 is a simplified outline of Part 8 of the Online Safety Bill. This simplified outline is included to assist readers to understand the substantive provisions of Part 8. However, the outline is not intended to be comprehensive. It is intended that readers should rely on the substantive provisions of Part 8.

Clause 72 – Children's Online Safety Special Account

Clause 72 establishes the Special Account (see subclause (1)).

Subclause (2) provides that the Special Account is a special account for purposes of the *Public Governance, Performance and Accountability Act 2013*.

The ACMA is to administer the Special Account (subclause (3)). An amount must not be debited from the Special Account without the Commissioner's written approval (subclause (4)).

Clause 73 – Credits to the Account

Clause 73 provides for the crediting of money to the Special Account.

Subclause (1) enables the Minister to determine that a specified amount be credited to the Special Account. If there is an appropriation for a departmental item that relates to the ACMA in an Appropriation Act, the Minister may, by writing, determine that a specified amount be debited against that appropriation and credited to the Special Account.

A determination made under subclause (1) is a legislative instrument, but is not subject to Parliamentary disallowance under section 42 of the *Legislative Instruments Act 2003* (subclause (2)). Exclusion from disallowance is appropriate in this instance to ensure certainty of funding to the Commissioner. This is similar to arrangements under section 44 of the *Legislative Instruments Act 2003*, which excludes instruments made under Appropriation Acts from disallowance.

For the purposes of the application of clause 73 to an Appropriation Act, the term 'ACMA departmental item' is defined to mean a departmental item (within the meaning of the Appropriation Act) that relates to the ACMA (subclause (3)).

Clause 74 – Purposes of the Account

Clause 74 sets out the purposes of the Special Account, which are:

- to enhance online safety for children;
- to make grants under paragraph 15(1)(g);

- to pay remuneration and other employment-related costs and expenses in respect of APS employees whose duties relate to the performance or exercise of the Commissioner's functions or powers;
- to pay any other costs, expenses and other obligations incurred by the Commonwealth in connection with the performance or exercise of the Commissioner's functions or powers; and
- to pay any costs, expenses and other obligations incurred by the Commonwealth under an agreement entered into under subclause 64(5).

The note to clause 74 draws the reader's attention to section 80 of the *Public Governance, Performance and Accountability Act 2013*, which deals generally with special accounts.

Part 9—Disclosure of information

Part 9 sets out the circumstances in which the Commissioner may disclose certain information, and the parties to which such information may be disclosed, including among others: the Minister, specified regulatory and law enforcements authorities, teachers, school principals and parents.

Clause 75 – Simplified outline of this Part

Clause 75 is a simplified outline of Part 9 of the Online Safety Bill. This simplified outline is included to assist readers to understand the substantive provisions of Part 9. However, the outline is not intended to be comprehensive. It is intended that readers should rely on the substantive provisions of Part 9.

The note to clause 75 cross-references clause 92 (which provides for referral of matters to law enforcement agencies).

Clause 76 – Scope

Clause 76 sets out the scope of Part 9, which applies to information obtained by the Commissioner through the exercise of powers, or performance of functions, conferred on the Commissioner by the Online Safety Bill or the BSA.

In dealing with the disclosures under this Part, it is expected that the Commissioner will be sensitive to privacy issues in disclosing information to other parties and will be expected to adopt appropriate procedures for the handling and disclosure of information about children.

Clause 77 – Disclosure to Minister

Clause 77 provides for the Commissioner to disclose information to the Minister.

Clause 78 – Disclosure to APS employees for advising the Minister

Clause 78 provides for the Commissioner to disclose information to the Secretary of the Minister's Department or an APS employee within that Department who is authorised by the Secretary.

Clause 79 – Disclosure to Royal Commissions

Clause 79 allows the Commissioner to disclose information to a Royal Commission, and to impose conditions in relation to such information.

Subclause (1) provides for the Commissioner to disclose information to a Royal Commission.

Subclause (2) allows the Commissioner to impose written conditions to be complied with in relation to information which has been disclosed to a Royal Commission. This is an important safeguard by which the Commissioner may limit further disclosure, where it is appropriate to do so.

Subclause (3) provides that an instrument under subclause 79(2) that imposes conditions relating to one particular disclosure is not a legislative instrument. Subclause (3) is declaratory of the law and is included to assist readers rather than create an exception to the *Legislative Instruments Act 2003*.

Subclause (4) provides that any other instrument under subclause 79(2) is a legislative instrument.

Clause 80 – Disclosure to certain authorities

Subclause 80(1) provides for the Commissioner to disclose information that will enable or assist an authority listed in paragraphs 80(1)(a) to (g), to perform or exercise any of the authority's function or powers. For example, the Commissioner might disclose information to the AFP under subclause 80(1) if satisfied that the information would assist the AFP to investigate a cybercrime offence under the Criminal Code.

The disclosures authorised under clause 80 are not intended to derogate from other authorised disclosures, such as the referral of matters to law enforcement agencies under clause 92 of the Online Safety Bill, clause 40 of Schedule 5 to the BSA or clause 69 of Schedule 7 to the BSA.

Subclause (2) allows the Commissioner to impose written conditions to be complied with in relation to information disclosed under subclause (1). This provides a safeguard by which the Commissioner may limit further disclosure of the information, where it is appropriate to do so.

Subclause (3) provides that an instrument under subclause 80(2) that imposes conditions relating to one particular disclosure is not a legislative instrument. Subclause (3) is declaratory of the law and is included to assist readers rather than create an exception to the *Legislative Instruments Act 2003*.

Subclause (4) provides that any other instrument under subclause 80(2) is a legislative instrument.

Clause 81 – Disclosure to teachers or school principals

Under subclause 81(1), the Commissioner may disclose information to a teacher or school principal if satisfied that the information will assist in the resolution of a complaint made under clause 18 of the Online Safety Bill. Where cyber-bullying involves a group of school students, involving the school may be the quickest and most effective means of resolving the complaint. The Commissioner will need to be able to disclose information to the school in these circumstances.

Subclause (2) allows the Commissioner to impose written conditions to be complied with in relation to information disclosed under subclause (1). For example, the Commissioner may impose a condition preventing secondary disclosures to third parties.

Subclause (3) provides that an instrument under subclause 81(2) that imposes conditions relating to one particular disclosure is not a legislative instrument. Subclause (3) is declaratory of the law and is included to assist readers rather than create an exception to the *Legislative Instruments Act 2003*.

Subclause (4) provides that any other instrument under subclause 81(2) imposing conditions is a legislative instrument.

Clause 82 – Disclosure to parents or guardians

Clause 82 enables the Commissioner to disclose information to a parent or guardian of an Australian child if the Commissioner is satisfied that the information will assist in the resolution of a complaint made under clause 18 of the Online Safety Bill.

Subclause (2) allows the Commissioner to impose written conditions to be complied with in relation to information disclosed under subclause (1). Such conditions may include a requirement preventing secondary disclosures to third parties.

Subclause (3) provides that an instrument under subclause 82(2) that imposes conditions relating to one particular disclosure is not a legislative instrument. Subclause (3) is declaratory of the law and is included to assist readers rather than create an exception to the *Legislative Instruments Act 2003*.

Subclause (4) provides that any other instrument under subclause 82(2) imposing conditions is a legislative instrument.

Clause 83 – Disclosure with consent

Clause 83 allows the Commissioner to disclose information that relates to the affairs of a person if the person has consented to the disclosure and the disclosure is in accordance with that consent.

Clause 84 – Disclosure of publicly available information

Clause 84 allows the Commissioner to disclose information that is already publicly available.

Clause 85 – Disclosure of summaries and statistics

Clause 85 allows the Commissioner to disclose summaries of de-identified information and statistics derived from de-identified information. The term ‘de-identified’ is defined in clause 4 of the Online Safety Bill.

Clause 86 – Relationship with Part 13 of the *Telecommunications Act 1997*

Clause 86 clarifies that the disclosures authorised by Part 9 do not authorise a disclosure of information that is prohibited by Part 13 of the Telecommunications Act, which regulates the use and disclosure of information obtained by certain bodies during the supply of telecommunication services.

Part 10—Miscellaneous

Part 10 deals with miscellaneous matters, such as review of decisions and legislative rules.

Clause 87 – Simplified outline of this Part

Clause 87 is a simplified outline of Part 10 of the Online Safety Bill. This simplified outline is included to assist readers to understand the substantive provisions of Part 10. However, the outline is not intended to be comprehensive. It is intended that readers should rely on the substantive provisions of Part 10.

Clause 88 – Review of decisions

Clause 88 provides for the review by the Administrative Appeals Tribunal (AAT) of certain decisions made by the the Commissioner, and sets out who may make an application for such review.

Subclause (1) provides for applications for review to be made to the AAT for a decision made under subclause 23(5) to refuse to declare a social media service as a tier 1 social media service, and under clause 25 to revoke a declaration of tier 1 status in relation to a social media service. Under subclause (2), any application made under subclause (1) may be made by the provider of the social media service concerned.

A decision to give a social media service notice to the provider of a social media service under clause 35 is reviewable under subclause 88(3). Subclause (4) limits who can make an application under subclause (3) to the provider of the social media service who received a notice under clause 35, or the end-user who posted the material the subject of the notice as these are the parties directly affected by the notice.

Under subclause (5), applications may be made to the AAT to review decisions made by the Commissioner refusing to give a social media service notice to a social media service. Subclause (6) limits who can make an application under subclause (5) to a person who made a complaint under clause 18 about the material the subject of the social media service notice, or the person who was the target of the material the subject of the social media service notice, or a person who has the consent of the person who was the target of the material the subject of the social media service notice.

Decisions by the Commissioner to give an end-user notice under clause 42 are reviewable under subclause (7). It is not proposed to enable merits review for decisions by the Commissioner to not issue an end-user notice. There will be a range of informal mechanisms available to the Commissioner for dealing with end-users, such as persuasion, negotiation, conciliation or referral to schools. Many complaints may be resolved without resort to the use of formal powers and generally it will be a preferred outcome for the Commissioner to use the least interventionist means available. It would not be appropriate to provide for merits review of decisions to not issue end-user notices in these circumstances.

Clause 89 – Protection from civil proceedings

Clause 89 provides for instances in which a person is protected from civil proceedings in relation to certain acts done in accordance with the Online Safety Bill or the BSA.

Subclause (1) prohibits civil proceedings from being brought against a person in respect of loss, damage or injury of any kind suffered by another person because of the following acts done in good faith:

- the making of a complaint under clause 18 (complaints about cyber-bullying material);
- the making of a statement to, or the giving of a document or information to, the Commissioner in connection with an investigation under clause 19.

Subclause 89(2) prohibits civil proceedings from being brought against a person in respect of acts done in compliance with a request under clause 29 (request for removal of cyber-bullying material), a social media service notice or an end-user notice.

Clause 90 – Liability for damages

Persons listed in paragraphs (a) to (c) of clause 90 are not liable to an action or other proceeding for damages for, or in relation to, an act or matter done or omitted to be done in good faith in:

- the performance or purported performance of any function; or
- in the exercise or purported exercise of any power;

  that is conferred on the Commissioner by or under the Online Safety Bill or the BSA.

Clause 91 – Protection from criminal proceedings—Commissioner etc.

The purpose of clause 91 is to protect from criminal proceedings persons whose powers and functions require them to do things in relation to material which would otherwise be prohibited. This provision is necessary to enable the protected persons to effectively perform their statutory functions.

Clause 91 provides protection from criminal liability for 'protected persons' (defined in subclause (1)) in relation to any of the acts listed in subclause (2) that were undertaken in connection with the exercise of a power, or the performance of a function, conferred on the Commissioner by or under the Online Safety Bill. This is intended to protect those delegated persons and body corporate entities who have undertaken activities as per subclause (2) in connection with exercise of a power or performance of a function conferred to them by the Commissioner.

For the purposes of clause 91, 'possession of material' as referred to in paragraph (2)(b) includes the custody or control of material, as clarified under subclause (3).

Clause 92 – Referral of matters to law enforcement agencies

The Commissioner may notify law enforcement agencies of particular material if he or she becomes aware of the particular material (through performance of a function or exercise of a power) that is of a sufficiently serious nature to warrant such referral and is not covered by clause 40 of Schedule 5 to the BSA or clause 69 of Schedule 7 to the BSA.

In those circumstances, the Commissioner may notify the material to a member of an Australian police force (defined in clause 4), or another person or body if there is an arrangement between the Commissioner and the chief (however described) of an

Australian police force under which the Commissioner is authorised to notify the content to that other person or body. The law enforcement agency officials that the Commissioner may refer the particular material to are listed in paragraphs 92(1)(d) and (e).

Subclause 92(2) provides an example of a manner by which material may be notified under paragraph (1)(d) to a member of the Australian police force (as defined in clause 4 to include the AFP and the police force of a State of Territory). Subclause 92(3) allows for the member of the Australian police force that has been notified of the particular material under clause 92 to notify the material to a member of another law enforcement agency.

If a member of the Australian Federal Police or of a State or Territory police force is notified of particular content under clause 92, that person may notify the content to a member of another law enforcement body in Australia or overseas (subclause 92(3)).

Subclause 92(4) provides that clause 92 does not, by implication, restrict the Commissioner's power to refer other matters to a member of the Australian police force. The Commissioner may choose, for example, to refer matters to a member of the Australian police force through powers vested in him or her in clause 80.

Clause 93 – Deferral of action in order to avoid prejudicing a criminal investigation

In certain cases, it is possible that a police investigation may be concurrent with a complaint to the Commissioner about particular material. As a safeguard, clause 93 provides that if a member of an Australian police force (as defined in clause 4) satisfies the Commissioner that taking an action under the Online Safety Bill in relation to material provided on a social media service or relevant electronic service would prejudice a criminal investigation, the Commissioner is entitled to defer taking that action until the end of a particular period of the criminal investigation.

Clause 94 – Copies of material

Clause 94 allows the Commissioner to make copies of material for the purposes of an investigation of a complaint under clause 19. Subclause (2) exempts the Commissioner from any copyright infringement if the Commissioner chooses to make copies of material under subclause (1).

Clause 95 – Compensation for acquisition of property

Clause 95 establishes a compensatory regime for acquisition of property under the Online Safety Bill. Subclause (1) sets out that the Commonwealth is liable to pay a reasonable amount of compensation if, within the meaning of paragraph 51(xxxi) of the Constitution, property was acquired from a person otherwise than on just terms (within the meaning of paragraph 51(xxxi) of the Constitution). Subclause 95(2) provides that if there is no agreement reached on the amount of compensation, then the person may commence proceedings in court for reasonable compensation as determined by the court.

Clause 96 – Service of notices by electronic means

Clause 96 disapplies paragraphs 9(1)(d) and (2)(d) of the *Electronic Transactions Act 1999* from applying to a notice under the Online Safety Bill or the Regulatory Powers Act, so far as that Act relates to the Online Safety Bill. Paragraphs 9(1)(d) and (2)(d)

of the *Electronic Transactions Act 1999* deal with the consent of the recipient of information to the information being given by way of electronic communication, and are not considered appropriate in circumstances where the Commissioner may frequently have access to electronic contact details only.

Clause 97 – Service of notices on contact person etc.

Clause 97 is a deeming provision setting out when a summons, process or notice is taken to have been served on, or given to, a provider of a social media service or to a body corporate incorporated outside Australia.

Subclause (2) provides that service of a required summons, process or notice on a provider of a social media service has taken place if served on or given to an individual that is an employee or agent of the provider and has been designated as the service's contact person for the purposes of the Online Safety Bill, and the individual's contact details have been notified to the Commissioner.

Subclause (3) provides that if a summons, process or notice is required to be served on, or given to a body corporate that is incorporated outside Australia, does not have a registered or principal office in Australia, and has an agent in Australia, the summons, process or notice can be served on, or given to, the agent of the body corporate in Australia.

Subclause (4) clarifies that subclauses (2) and (3) have effect in addition to section 28A of the *Acts Interpretation Act 1901* which deals with the service of documents.

Clause 98 – This Act does not limit Schedule 5 or 7 to the *Broadcasting Services Act 1992*

Clause 98 clarifies that the Online Safety Bill does not limit the operation of Schedules 5 or 7 to the BSA.

Clause 99 – This Act does not limit the *Telecommunications Act 1997*

Clause 99 clarifies that the Online Safety Bill does not limit the operation of the Telecommunications Act.

Clause 100 – Implied freedom of political communication

Clause 100 is a constitutional safeguard, which provides that the Online Safety Bill does not apply to the extent (if any) that it would infringe any constitutional doctrine of implied freedom of political communication.

This clause does not limit the application of section 15A of the *Acts Interpretation Act 1901* to the Online Safety Bill. That section provides that every Act shall be read and construed subject to the Constitution.

Clause 101 – Concurrent operation of State and Territory laws

In accordance with clause 101, it is the intention of Parliament that the Online Safety Bill does not apply to the exclusion of a law of a State or Territory, to the extent to which that law is capable of operating concurrently.

Clause 101 is intended to ensure that different Commonwealth and State/Territory laws that address aspects of cyber-bullying will operate concurrently with one another.

Clause 102 – This Act not to affect performance of State or Territory functions

Clause 102 is also a constitutional safeguard. It provides that a power conferred by this Bill must not be exercised in such a way as to prevent the exercise of the powers, or the performance of the functions, of government of a State, the Northern Territory, the Australian Capital Territory or Norfolk Island.

Clause 103 – Revocation or variation of instruments

Subsection 33(3) of the *Acts Interpretation Act 1901* provides that, where an Act confers a power to make, grant or issue any instrument of a legislative or administrative character, the power shall be construed as including a power exercisable in the like manner and subject to the like conditions (if any) to, relevantly, revoke or vary any such instrument.

Various clauses of the Online Safety Bill permit the making of instruments of this nature, and expressly provide for the revocation and variation of instruments so made. Clause 103 provides that a provision of the Online Safety Bill that expressly authorises the revocation or variation of an instrument does not, by implication, limit the application of subsection 33(3) of the *Acts Interpretation Act 1901* in relation to other instruments under this Act.

This clause operates to put beyond doubt that, notwithstanding the presence of certain express variation and revocation provisions in the Online Safety Bill, subsection 33(3) of the *Acts Interpretation Act 1901* continues to apply in relation to other instruments under the Online Safety Bill.

Clause 104 –Terms of use of a social media service

Clause 104 clarifies when terms of use of a social media service may be regarded as the equivalent of a provision that prohibits end-users from posting cyber-bullying material. The issue of when terms of use will be considered equivalent is relevant to ascertaining whether a social media service meets the basic online safety requirements, under clause 21, and also to application of the 'special rule' in relation to a request for removal of cyber-bullying material under clause 29.

Terms of use which do not expressly prohibit end-users from posting on the social media service cyber-bullying material targeted at an Australian child, but which have the same effect, may be reasonably regarded as equivalent.

Subclause (2) clarifies that, for the purposes of clause 104, the ordinary meaning of 'cyber-bullying material' applies.

Clause 105 – Provider of social media service or relevant electronic service

Clause 105 is an interpretive provision. The expressions 'social media service' and 'relevant electronic service' are defined in clause 4, and several provisions of the Online Safety Bill refer to such services. Clause 105 provides that, for the purposes of the Online Safety Bill, a person does not provide a social media service or relevant electronic service merely because the person:

- supplies a carriage service that enables material to be accessed or delivered, or
- provides a billing service, or a fee collection service, in relation to a social media service or relevant electronic service.

Clause 106 – Extended meaning of use

Clause 106 is an interpretative provision. It provides that, unless the contrary intention appears, a reference, in the Online Safety Bill, to the 'use' of a thing is a reference to the use of the thing either in isolation or in conjunction with one or more other things.

Clause 106 is based on of clause 17 of Schedule 7 to the BSA, and is intended to overcome potential difficulties in attributing instrumentality to a single element of a system, where the whole system is required to perform an act.

Clause 107 – Review of this Act etc.

Clause 107 requires that within 3 years after the commencement of this clause, the Minister must cause a review to be conducted of the operation of the *Enhancing Online Safety for Children Act 2014* and the legislative rules (clause 108) and whether any amendments to the Act or the rules are required.

The review must also consider whether a delegation should be made to a body corporate under subclause 64(1) (under which the Commissioner is able to delegate certain powers to a company limited by guarantee specified in the legislative rules).

Subclause (2) requires the Minister to cause to be prepared a report of this review, and after completion of the report, for copies of the report to be tabled in each House of Parliament within 15 sitting days of that House.

Clause 108 – Legislative rules

Clause 108 is a standard provision which permits the Minister to make legislative rules for the purposes of the Online Safety Bill, subject to the exclusions set out in subclause 108(2).

ENHANCING ONLINE SAFETY FOR CHILDREN (CONSEQUENTIAL AMENDMENTS) BILL 2014

Clause 1 – Short title

Clause 1 provides that the Consequential Amendments Bill, when enacted, may be cited as the *Enhancing Online Safety for Children (Consequential Amendments) Act 2014*.

Clause 2 – Commencement

Clause 2 provides for the commencement of the Consequential Amendments Bill.

Clauses 1 to 3 of the Consequential Amendments Bill and anything else not covered in the table at subclause (1) will commence on the day of Royal Assent.

Part 1 of Schedule 1, Part 1 of Schedule 2 and Schedule 3 will commence at the same time as clause 3 of the Online Safety Bill. Clause 3 of the Online Safety Bill commences on a date to be fixed by Proclamation under clause 2 of that Bill. However, if clause 3 does not commence within the period of 6 months beginning on the day of Royal Assent of that Bill, it commences on the day after the end of that period.

Part 2 of Schedule 1 will commence immediately after the commencement of Part 1 of Schedule 1, the commencement of which is outlined above.

Part 2 of Schedule 2 will commence immediately after the commencement of Part 3 of Schedule 1 to the *Telecommunications Legislation Amendment (Deregulation) Act 2014* (the Telecommunications Deregulation Act), noting the possible effect of clause 4 on the reference to the title of this Act.

However, if Part 3 of Schedule 1 to the Telecommunications Deregulation Act commences before the commencement of Part 1 of Schedule 2 of the Consequential Amendments Bill, Part 2 of Schedule 2 will not commence at all. The reason for this is outlined at the note for Part 2 of Schedule 2 below. The commencement of Part 1 of Schedule 2 of the Consequential Amendments Bill is outlined above.

Clause 3 – Schedules

Clause 3 provides that legislation that is specified in a Schedule to the Consequential Amendments Bill is amended or repealed as set out in the applicable items in that Schedule, and any other item in a Schedule has effect according to its terms. There are three Schedules to this Bill.

The items in Schedules 1 and 2 make amendments consequential to the Online Safety Bill, and reflect the new functions of the Commissioner. The Schedules amend the following Acts:

- the ACMA Act
- the BSA
- the Criminal Code
- the FOI Act

- the Telecommunications Act

Schedule 3 contains transitional provisions relating to the amendments made by the Consequential Amendments Bill and the enactment of the Online Safety Bill.

Clause 4 – Translation of certain references

Clause 4 translates references to the Telecommunications Deregulation Act in the Online Safety Bill if the Telecommunications Legislation Amendment (Deregulation) Bill 2014 is not enacted until 2015, where it would instead need to be cited as the *Telecommunications Legislation Amendment (Deregulation) Act 2015*.

Schedule 1—Amendments of the Broadcasting Services Act 1992

Schedule 1 amends the BSA to transfer relevant functions and powers for the administration of the Online Content Scheme in Schedules 5 and 7 to the BSA from the ACMA to the Commissioner, and to provide powers for the Commissioner relating to its functions under the Online Safety Bill.

Part 1—General amendments

Part 1 of Schedule 1 to the Consequential Amendments Bill deals with general amendments to the BSA for the purpose described above.

Part 13 of the BSA provides the ACMA with information gathering powers. Items 2 to 15 of Part 1 of Schedule 1 amend Part 13 of the BSA to reflect the transfer of the power to conduct specific investigations relating to the Online Content Scheme from the ACMA to the Commissioner. They also apply Part 13 to investigations conducted by the Commissioner under the Online Safety Bill.

Items 16 to 23 amend Schedule 5 to the BSA and Items 24 to 35 amend Schedule 7 to the BSA to reflect the transfer of the administration of Schedules 5 and 7 to the BSA from the ACMA to the Commissioner.

Broadcasting Services Act 1992

Item 1 – Subsection 6(1)

Item 1 inserts a definition of Commissioner into subsection 6(1) of the BSA, providing that the Commissioner is the Children's e-Safety Commissioner established under the Online Safety Bill.

Item 2 – Part 13 (heading)

Item 2 repeals the heading of Part 13 of the BSA 'Information gathering by the ACMA' and substitutes the replacement heading 'Information gathering by the ACMA and the Commissioner' to add a reference to the Commissioner's powers under this Part.

Item 3 – At the end of Division 1 of Part 13

Division 1 of Part 13 of the BSA creates introductory provisions for Part 13, which previously only applied to information gathering by the ACMA, including investigations conducted by it. Item 3 inserts new section 169A at the end of Division 1 of Part 13, to distinguish that an 'investigation' by the Commissioner is limited to an investigation conducted under clause 19 of the Online Safety Bill, clause 27 of Schedule 5 to the BSA or clause 44 of Schedule 7 to the BSA.

Item 4 – Section 173
Item 5 – Section 173
Item 6 – At the end of section 173

Section 173 of the BSA empowers the ACMA to give a written notice summoning a person to give evidence regarding an investigation. Items 4 to 6 amend section 173, adding new subsection 173(2) to provide equivalent powers to the Commissioner in

respect of investigations conducted under the Online Safety Bill or Schedules 5 or 7 to the BSA.

Item 7 – Before subsection 174(1)
Item 8 – At the end of section 174

Section 174 of the BSA empowers a delegate of the ACMA to require a person summoned to give evidence for an investigation to be examined under affirmation or oath that the person will make statements true to the best of the person's knowledge. Items 7 and 8 amend section 174. Item 7 inserts a new subheading. Item 8 adds new subsections 174(4) to (6) to provide equivalent powers in respect of investigations conducted by the Commissioner or a delegate of the Commissioner.

Item 9 – Before subsection 176(1)
Item 10 – At the end of section 176

Section 176 of the BSA requires a record to be taken of an ACMA delegate's examination of a person during an investigation, and entitles that person to be given a copy of that record. Items 9 and 10 amend section 176. Item 9 inserts a new subheading. Item 10 adds new subsections 176(3) and (4) to provide equivalent requirements for examinations of persons during investigations conducted by the Commissioner or a delegate of the Commissioner.

Item 11 – Section 177
Item 12 – Paragraph 177(a)
Item 13 – At the end of section 177

Section 177 of the BSA empowers the ACMA to give a written notice requiring a person to make documents in the possession of the person available to the ACMA that may contain information relevant to the subject matter of an investigation. The person must also permit the ACMA to make copies of those documents. Items 11 to 13 amend section 177. Items 11 and 12 make consequential amendments. Item 13 adds new subsection 177(2) to provide equivalent powers in respect of investigations conducted by the Commissioner or a delegate of the Commissioner.

Item 14 – Subsection 200(3)
Item 15 – At the end of section 200

Subsection 200(3) of the BSA provides the same protections afforded to a witness in a proceeding in the High Court to persons who appear at a hearing, give evidence or produce document at an investigation or hearing conducted or held by the ACMA. Items 14 and 15 amend section 200. Item 14 makes a consequential amendment. Item 15 adds new subsection 200(4) to give the same protections to persons who give evidence or produce documents at an investigation conducted by the Commissioner.

Item 16 – Clause 27 of Schedule 5
Item 17 – Subclause 28(2) of Schedule 5
Item 18 – Subclause 68(5) of Schedule 5
Item 19 – Subclause 69(4) of Schedule 5
Item 20 – Subclause 70(8) of Schedule 5
Item 21 – Subclause 71(8) of Schedule 5
Item 22 – Clause 74 of Schedule 5
Item 23 – Paragraph 94(f) of Schedule 5
Item 24 – Clause 44 of Schedule 7
Item 25 – Subclause 45(2) of Schedule 7
Item 26 – Subclause 91(4) of Schedule 7
Item 27 – Subclause 92(3) of Schedule 7
Item 28 – Subclause 93(7) of Schedule 7
Item 29 – Subclause 94(7) of Schedule 7
Item 30 – Clause 97 of Schedule 7
Item 31 – Paragraph 112(1)(b) of Schedule 7
Item 32 – Paragraph 112(1)(d) of Schedule 7
Item 33 – Paragraph 112(1)(e) of Schedule 7
Item 34 – Paragraph 114(f) of Schedule 7
Item 35 – Subclause 115(3) of Schedule 7

Schedules 5 and 7 to the BSA contain a variety of references to powers and responsibilities of the ACMA, which are to be transferred to the Commissioner.

Items 16 to 35 amend various provisions in these Schedules to replace references to the ACMA with references to the Commissioner, or make other similar amendments. In particular, item 31 repeals paragraph 112(1)(b) as there is no equivalent class of persons to members or associate members of the ACMA and item 32 replaces a reference to consultants under paragraph 112(1)(d) with consultants engaged under clause 69 of the Online Safety Bill.

Part 2—Amendments to change certain references to the ACMA into references to the Commissioner

Broadcasting Services Act 1992

Item 36 – Amendments—changing certain references to the ACMA into references of the Commissioner
Item 37 – Schedule 5
Item 38 – Schedule 7 (other than paragraphs (a) and (b) of the definition of *licensed broadcasting service* in clause 2, subparagraph 9A(1)(a)(ii) and paragraphs 112(1)(c) and (e))

Similarly to items 16 to 35 above, items 36 to 38 amend Schedules 5 and 7 to the BSA to replace the remaining references to the ACMA with references to the Commissioner. However, in Schedule 7, the references to the ACMA are retained in paragraphs (a) and (b) of the definition of ***licensed broadcasting service*** in clause 2, in subparagraph 9A(1)(a)(ii) and in paragraphs 112(1)(c) and (e).

Schedule 2—Amendments of other Acts

Schedule 2 amends the ACMA Act, the Criminal Code, the FOI Act and the Telecommunications Act consequential to the transfer of relevant functions and powers for the administration of the Online Content Scheme in Schedules 5 and 7 to the BSA from the ACMA to the Commissioner.

Part 1—General amendments

Australian Communications and Media Authority Act 2005

Part 1 of Schedule 2 amends the ACMA Act to:

- reflect the office of the Children's e-Safety Commissioner as an independent statutory office residing within the ACMA; and
- limit the ACMA's functions in relation to internet content to reflect the Commissioner's responsibility for those matters that fall within the Commissioner's functions; and
- require the ACMA to include in the ACMA's annual report, details of the ACMA's expenditure on the Commissioner's functions.

It also makes consequential amendments to the Criminal Code, the FOI Act and the Telecommunications Act.

Item 1 – Section 3 (subparagraph (b)(iia) of the definition of *authorised disclosure information*)
Item 2 – Section 3 (paragraph (c) of the definition of *investigation*)

Items 1 and 2 amend the definitions of ***authorised disclosure information*** and ***investigation*** in section 3 of the ACMA Act to remove references to Schedules 5 and 7 to the BSA. These amendments reflect the transfer of functions and powers under those Schedules from the ACMA to the Commissioner.

Item 3 – Paragraph 4(3)(b)

Section 4 of the ACMA Act defines when an inquiry, investigation or hearing ***ends*** for the purposes of that Act. Item 3 amends paragraph 4(3)(b) to remove references to provisions in Schedules 5 and 7 to the BSA, as a consequence of the functions and powers under those Schedules being transferred from the ACMA to the Commissioner.

Item 4 – Paragraph 10(1)(a)
Item 5 – Subparagraph 10(1)(o)(ii)

Subsection 10(1) of the ACMA Act sets out the ACMA's ***broadcasting, content and datacasting functions***. Items 4 and 5 amend subsection 10(1) to remove functions relating to the online content scheme under the BSA or Schedules 5 or 7 to the BSA. These amendments reflect the transfer of these functions from the ACMA to the Commissioner, as provided for in clause 15 of the Online Safety Bill.

Item 6 – Paragraphs 53(2)(n), (o), (p) and (pa)

Subsection 53(2) of the ACMA Act prohibits the ACMA from delegating certain powers under the BSA through its delegation powers under sections 51 and 52 of the ACMA Act. Item 6 repeals paragraphs 53(2)(n), (o), (p) and (pa) of the ACMA Act that prohibit delegation of powers under Schedules 5 and 7 to the BSA relating to powers to formulate specific schemes or to determine specific standards or determinations. These amendments are consequential to the functions and powers under those Schedules being transferred from the ACMA to the Commissioner.

Item 7 – After paragraph 57(a)

Section 57 of the ACMA Act outlines the required components of the annual report prepared by the Chair of the ACMA under section 46 of the *Public Governance, Performance and Accountability Act 2013*. Item 7 amends section 57, adding new paragraph 57(aa). This paragraph requires the ACMA in its annual report to include details of employment-related costs for staff performing duties relating to the Commissioner's functions and powers, as well as other expenditure incurred by the Commonwealth on the Commissioner's functions and powers.

Item 8 – After paragraph 59D(1)(l)

Section 59D of the ACMA Act empowers an ACMA official, where authorised in writing by the ACMA Chair, to disclose authorised disclosure information to specific authorities specified in subsection 59D(1). Item 8 amends subsection 59D(1), adding new paragraph 59D(1)(la) to allow disclosure of such information to be made to the Commissioner.

Criminal Code Act 1995

Item 9 – Paragraph 273.9(5)(a) of the Criminal Code
Item 10 – Paragraph 273.9(5)(a) of the Criminal Code
Item 11 – Paragraph 474.21(4)(a) of the Criminal Code
Item 12 – Paragraph 474.21(4)(a) of the Criminal Code
Item 13 – Paragraph 474.24(4)(a) of the Criminal Code
Item 14 – Paragraph 474.24(4)(a) of the Criminal Code

The Criminal Code establishes certain offences for crimes relating to child pornography, such as possession, production, distribution etc. of child pornography (Division 273) or using a carriage service for child pornography material (Subdivision D of Division 474).

Paragraphs 273.9(5)(a) and 474.21(4)(a) also provides defences for persons who might otherwise be criminally liable for certain crimes under the above Divisions while engaging with child pornography materials in good-faith for the sole purpose of assisting the ACMA to detect prohibited content or potential prohibited content for the purposes of Schedules 5 and 7 to the BSA.

Items 9 to 14 replace references to the ACMA with references to the Commissioner, consequential to the transfer of the functions and powers under Schedules 5 and 7 to the BSA from the ACMA to the Commissioner.

Freedom of Information Act 1982

Item 15 – Division 1 of Part II of Schedule 2 (before the item relating to the Classification Board)

Subsection 7(2) of the FOI Act exempts certain documents held by certain persons, bodies and entities from the application of the FOI Act. Division 1 of Part II of Schedule 2 lists the exempted bodies' documents. Item 15 amends this division to add an exemption for the Children's e-Safety Commissioner. This exempts the Commissioner from releasing to the public particular content-service documents or internet-service documents relating to the performance of a function, or the exercise of a power under Schedules 5 and 7 of the BSA.

Telecommunications Act 1997

Item 16 – Section 284 (heading)
Item 17 – After subsection 284(1)

Part 13 of the Telecommunications Act provides a framework for the protection of information relating to communications. Section 284 of the Telecommunications Act provides exceptions for eligible persons and eligible number-database persons, as listed in sections 271 and 272 of that Act, from the prohibition of disclosing certain types of information or documents specified under sections 276 and 277.

Items 16 and 17 amend section 284. Item 16 substitutes a new heading. Item 17 adds new subsection 284(1A) to provide an additional exception to sections 276 and 277. This exception allows eligible persons and eligible number-database persons to disclose information or a document to the Commissioner or an ACMA staff member whose duties relate to the performance of the Commissioner's functions where that information or document may assist the Commissioner in carrying out his or her functions or powers.

Item 18 – Section 299 (heading)
Item 19 – After subsection 299(1)
Item 20 – Section 299 (note)

Section 299 provides that if information or a document is disclosed to a person under section 284 of the Telecommunications Act, the person must not disclose or use the information or document except for the purpose of, or in connection with, the carrying out of the functions and powers of the relevant agency listed in section 284 (e.g. the ACMA in subsection 299(1) and 284(1)).

Items 18 to 20 amend section 299. Item 19 inserts new subsection 299(1A) to provide a similar secondary disclosure/use provision in relation to information or a document disclosed to the Commissioner under new subsection 284(1A) (see items 16 and 17, above). Items 18 and 20 update the section 299 heading and note to include a reference to the Commissioner.

Item 21 – Part 34 (heading)
Item 22 – At the end of section 579
Item 23 – After subsection 581(2)
Item 24 – After subsection 581(4)

Part 34 deals with special provisions relating to functions and powers of the ACMA and the Attorney-General in respect of telecommunications. Within Part 34, section 581 deals with the ACMA's power to give written directions to carriers or service providers in connection with performing or exercising any of the ACMA's telecommunications functions or powers.

Items 23 and 24 amend section 581, adding new subsections 581(2A), (2B) and (4A) to also allow the Commissioner to give written directions to carriers or service providers in connection with his or her functions or powers. Carriers or service providers must comply with such directions.

Items 21 and 22 make consequential amendments to the heading and simplified outline of Part 34 to reflect these new powers.

Part 2—Amendments contingent on the commencement of the *Telecommunications Legislation Amendment (Deregulation) Act 2014*

The following amendments are contingent upon the date of commencement of the Telecommunications Deregulation Act. These items commence immediately after Part 3 of Schedule 1 to that Act if it has not commenced before Part 1 of Schedule 2 to the Consequential Amendment Bill. Otherwise, these items do not commence at all.

Part 3 of Schedule 1 to the Telecommunications Legislation Amendment (Deregulation) Bill 2014, if enacted, would repeal and replace the headings of sections 284 and 299 and the note to section 299 of the Telecommunications Act. Similarly, items 16, 18 and 20 in Part 1 of Schedule 2 to the Consequential Amendments Bill also repeal and replace these headings and notes.

This Part preserves the amendments made by items 16, 18 and 20 above in the event that Part 3 of Schedule 1 to Telecommunications Deregulation Act commences after Part 1 of Schedule 2 to the Consequential Amendments Bill.

Telecommunications Act 1997

Item 25 – Section 284 (heading)

Item 25 remakes the amendment made by item 16 of Schedule 2 to the heading of section 284 in the event that Part 3 of Schedule 1 to Telecommunications Deregulation Act commences after Part 1 of Schedule 2 to the Consequential Amendments Bill.

Item 26 – Section 299 (heading)
Item 27 – Section 299 (note)

Items 26 and 27 remake the amendments made by items 18 and 20 of Schedule 2 to the section 299 heading and note in the event that Part 3 of Schedule 1 to Telecommunications Deregulation Act commences after Part 1 of Schedule 2 to the Consequential Amendments Bill.

Schedule 3— Transitional provisions

Schedule 3 contains transitional provisions relating to the amendments made by the Consequential Amendments Bill and the enactment of the Online Safety Bill.

Item 1 – Definitions

Item 1 of Schedule 3 defines key terms used in Schedule 3. Notably, it defines ***transition time*** to mean the commencement of Schedule 3, which commences at the same time as clause 3 of the Online Safety Bill.

Item 2 – Transitional—acts of the ACMA to be attributed to the Commissioner

Item 2 provides that anything done by, or in relation to, the ACMA before the transition time under, or for the purposes of, Schedules 5 or 7 to the BSA, has effect as if it were done by, or in relation to, the Commissioner. This ensures continuity after the transfer of responsibility for the administration of Schedules 5 and 7 to the BSA from the ACMA to the Commissioner.

Item 3 – Substitution of Commissioner as a party to certain pending proceedings

Item 3 substitutes the Commissioner for the ACMA as a party to any proceedings under, or in connection with, Schedule 5 or 7 to the BSA which were pending in any court or tribunal immediately before the transition time and to which the ACMA was a party.

Item 4 – Transitional—transfer of records to the Commissioner

Item 4 applies to any records or documents in possession of the ACMA immediately before the transition time which wholly or partly concern Schedule 5 or 7 to the BSA.

Subitem 4(2) provides that if the records or documents wholly concern Schedule 5 or 7 they are to be transferred to the Commissioner after the transition time.

Subitem 4(3) provides that if the records or documents partly concern Schedule 5 or 7, they are to be made available to the Commissioner at the Commissioner's request.

Item 5 – Transitional—authorised disclosure information

Item 5 preserves the unamended version of the definition of ***authorised disclosure information*** for information obtained by the ACMA prior to the transition time. The amendment of the definition of ***authorised disclosure information*** is discussed in the notes on item 1 of Schedule 2.

Item 6 – Transitional—protection from civil proceedings

Item 6 preserves the unamended versions of clause 29 of Schedule 5 to the BSA and clause 46 of Schedule 7 to the BSA in relation to anything done before the transition time. These clauses are amended by Part 2 of Schedule 1.

Clause 29 of Schedule 5 and clause 46 of Schedule 7 to the BSA provide protection from civil proceedings in certain circumstances.

Item 7 – Transitional—protection from criminal proceedings

Item 7 preserves the unamended version of clause 112 of Schedule 7 to the BSA in relation to anything done before the transition time by the ACMA and the other persons specified in the item. Clause 112 is amended by Schedule 1.

Item 8 – Transitional rules

Item 8 allows the Minister to make rules, by legislative instrument, in relation to transitional matters arising out of either or both the amendments made by the Consequential Amendments Bill and the enactment of the Online Safety Bill.