Reviews of the *Enhancing Online Safety Act 2015* and the Online Content Scheme—discussion paper

June 2018

Disclaimer

The material in this paper is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances. The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this paper.

This paper has been prepared for consultation purposes only and does not indicate the Commonwealth's commitment to a particular course of action. Additionally, any third party views or recommendations included in this paper do not reflect the views of the Commonwealth, or indicate its commitment to a particular course of action.

Copyright

© Commonwealth of Australia 2018


The material in this paper is licensed under a Creative Commons Attribution—4.0 International licence, with the exception of:

- the Commonwealth Coat of Arms
- this Department's logo
- any third party material
- any material protected by a trademark, and
- any images and/or photographs.

More information on this CC BY licence is set out as follows:

- Creative Commons website—www.creativecommons.org
- Attribution 4.0 international (CC by 4.0)—www.creativecommons.org/licenses/by/4.0.

Enquiries about this licence and any use of this discussion paper can be sent to: copyright@communications.gov.au.

Third party copyright

The Department of Communications and the Arts (the Department) has made all reasonable efforts to clearly identify material where the copyright is owned by a third party. Permission may need to be obtained from third parties to re-use their material.

Attribution

The CC BY licence is a standard form licence agreement that allows you to copy and redistribute the material in any medium or format, as well as remix, transform, and build upon the material, on the condition that you provide a link to the licence, you indicate if changes were made, and you attribute the material as follows:

> Licensed from the Commonwealth of Australia under a Creative Commons Attribution 4.0 International licence.

Enquiries about the use of any material in this publication can be sent to: copyright@communications.gov.au.

Using the Commonwealth Coat of Arms

Guidelines for using the Commonwealth Coat of Arms are available from the Department of the Prime Minister and Cabinet website at www.pmc.gov.au/government/its-honour.

Contents

Introduction

Context for this discussion paper

Australians are immersing themselves in the online world through social networking sites, online gaming, search engines, applications and other media and content services. The internet is a vital tool for education, innovation and business, research, entertainment and social interaction in a modern day society. Faster broadband connections, the digitisation of content, both commercial and user-generated, and the proliferation of connected devices, such as smartphones and tablets, has given Australians access to a greater amount of online content than ever before.

While this has created exciting opportunities for users and business, it has also brought about many challenges and concerns for regulators, including a lack of control over content on the internet that may lead to increased opportunity for illegal and antisocial activities.

An unfortunate consequence is that this can leave Australians, in particular children and teenagers, vulnerable to harmful behaviours and socially unacceptable content. The online safety space is a rapidly changing environment that incorporates a number of wide ranging issues. Issues include cyberbullying, pornography, image-based abuse (IBA), violence against women, violent extremism, and child sexual abuse. In extreme circumstances, some of these can lead to terrible outcomes including radicalisation, severe distress, mental health issues and even death.

In 2015, the Australian Government established the Office of the Children's eSafety Commissioner under the *Enhancing Online Safety for Children Act 2015* to help protect Australian children from cyberbullying harm and to take a national leadership role in online safety for children. In 2017, the Government expanded the Commissioner's remit to cover online safety for all Australians. The office was renamed the Office of the eSafety Commissioner (eSafety Commissioner), and the legislation as the *Enhancing Online Safety Act 2015* (the Online Safety Act)[1]. Section 107 of the Online Safety Act requires that the operation of the Act be reviewed by the Government within three years after its commencement (the Statutory Review of the Act).

The eSafety Commissioner also administers Schedules 5 and 7 to the *Broadcasting Services Act 1992* (BSA) (known as the Online Content Scheme)[2]. The Government considers it best to conduct a review of the Online Content Scheme at the same time as the Statutory Review of the Act. This approach will allow related aspects of the Government's online safety regulatory framework to be considered at once and will ensure that any recommendations made are comprehensive and support an efficient and effective overall outcome. It is important that Australia has the proper regulatory controls and support systems in place to mitigate online risks and ensure that Australians can confidently take advantage of the benefits of the internet and the digital environment.

These Reviews will be conducted by an independent reviewer, who will prepare a report for consideration by the Minister for Communications. The final report will be tabled in Parliament.

This discussion paper is the starting point of these two Reviews inviting stakeholders and interested parties to provide to the Department, by written submission, their views about:

- the Online Safety Act, which establishes the eSafety Commissioner and sets out the powers, functions and governance arrangements, and
- the Online Content Scheme in Schedules 5 and 7 to the BSA, which regulates the internet industry and content services industry in relation to prohibited and potentially prohibited content.

Terms of Reference

The complete Terms of Reference for the two Reviews are below.

Statutory Review of the Enhancing Online Safety Act 2015

The Terms of Reference of this Review are prescribed in Section 107 of the Act which requires a review of the following matters be conducted:

- the operation of the Act and the legislative rules;
- whether the Act or the legislative rules should be amended, and
- whether a delegation should be made under subsection 64 (1) of the Act (Delegation by the Commissioner to a body corporate).

Subsection 64 (1) of the Act states:

64 Delegation by the Commissioner to a body corporate

The Commissioner may, by writing, delegate any or all of the Commissioner's functions or powers under:

a) Part 3; or
b) Part 4 (other than section 35 or 37)
to a body corporate that is:
c) Specified in the legislative rules, and
d) A company that is registered under Part 2A.2 of the *Corporations Act 2001*, and
e) A company limited by guarantee.

The specific elements to be examined by the Review will include:

- the extent to which the policy objectives and provisions of the Act remain appropriate for the achievement of the Government's current online safety policy intent
- the Commissioner's remit, including roles and responsibilities, and whether the current functions and powers in the Act are sufficient to allow the Commissioner to perform his/her job effectively;
- whether the current governance structure and support arrangements for the Commissioner provided by the ACMA are fit for purpose; and
- whether legislative change is required to allow the Commissioner to perform his/her functions and powers more effectively.

Schedules 5 and 7 to the Broadcasting Services Act 1992

The Review of Schedules 5 and 7 to the *Broadcasting Services Act 1992* (Online Content Scheme) will examine the operation of the Online Content Scheme, including the following matters:

a) the relevance and effectiveness of the Online Content Scheme in the context of the contemporary communications environment and modern consumption patterns of online media and services
b) the scope of regulation, including whether the Online Content Scheme's link to the National Classification Scheme categories (MA 15+, R 18+, X 18+ and RC) is still effective
c) the most effective balance of tools available for dealing with prohibited online content, including legislation, co-regulatory schemes, self-regulatory schemes and technical protections, and
d) an assessment of other regimes, including international models, in dealing with prohibited content that is hosted overseas.

About online safety

In 2015, the Australian Government implemented measures to create a safer online environment for Australian children. The key measure was the establishment of the Office of the Children's eSafety Commissioner, under the *Enhancing Online Safety for Children Act 2015*, to help protect Australian children from cyberbullying harm and to take a national leadership role in online safety for children.

In December 2015, the functions of the Children's eSafety Commissioner were expanded through legislative rules[3] to include online safety for persons at risk of family or domestic violence. At the 2016 Federal election, the Government also made a number of election commitments relating to ensuring online safety for women and senior Australians. Some of these measures were implemented by the Children's eSafety Commissioner, including the national online complaints portal to help counter the effects of the non-consensual sharing of intimate images, and an online seniors portal and outreach programs to support, coach and teach older Australians to improve their skills and give them greater confidence in using digital technology.

In order to implement a statutory basis to this range of functions, the *Enhancing Online Safety for Children Act 2015* was amended on 23 June 2017. The Explanatory Memorandum to the amending legislation noted that the changes would "reflect the broader role for online safety that the Commissioner has that goes beyond online safety for Australian children. This broader role includes functions in relation to persons at risk of family or domestic violence, in relation to victims of the non-consensual sharing of intimate images, and in relation to the safe use of the internet by older Australians."[4] The expansion of the role related to the eSafety Commissioner's 'soft functions' set out at section 15 of the Act (e.g. promotional activities, research, advice). The cyberbullying complaints scheme administered by the eSafety Commissioner remained confined to material targeted at Australian children.

About the eSafety Commissioner

The eSafety Commissioner is an independent statutory office, supported by the Australian Communications and Media Authority (ACMA). The current eSafety Commissioner, Ms Julie Inman-Grant, was appointed in January 2017 for a five year term.

The eSafety Commissioner works to promote online safety for all Australians, particularly children, by undertaking research, coordinating relevant online safety activities of Commonwealth Departments, authorities and agencies, and acting as Chair of the Government's Online Safety Consultative Working Group (OSCWG).

The eSafety Commissioner also administers a complaints system for cyberbullying material, comprising the Rapid Removal Scheme for large social media services and the End-user Notice Regime (explained in more detail later in this discussion paper), and the Online Content Scheme, a complaints system for prohibited online content (explained in more detail later in this discussion paper). These schemes aim to limit the availability of certain content online and safeguard children from harmful or inappropriate content.

The eSafety Commissioner also has an important role in educating Australians about managing technology risks and protecting themselves and their personal information online, using technology and sharing content responsibly, and providing avenues for support and assistance.

Recent reviews relevant to online safety

In November 2016, the Senate References Committee on Environment and Communications released its report on the *Harm being done to Australian children through access to pornography on the Internet.*[5] On 20 April 2017, the Government tabled its response and, as a result, a panel of experts was convened from within the OSCWG to consider the issue and make recommendations to address the issue of the harms associated with children's access to online pornography. The group continues to provide advice to Government in relation to online pornography, and a broader range of online safety matters, and this advice will inform future policy decisions.

In October 2017, the Senate Legal and Constitutional Affairs References Committee (Committee) commenced an inquiry into the adequacy of existing offences in the Commonwealth Criminal Code and of state and territory criminal laws to capture cyberbullying. This inquiry examined, among other things, the adequacy of existing policies, procedures and practices of social media platforms in preventing and addressing cyberbullying and the application of section 474.17 of the Commonwealth Criminal Code and the adequacy of the penalty, particularly where the victim of cyberbullying has self-harmed or died by suicide. The Committee tabled its report on 28 March 2018.[6]

- The Committee recommended a broad package of Government reforms including in relation to imposing a social media duty of care. It recommended the Government:
- ensure that the eSafety Commissioner is adequately resourced to fulfil all its functions, taking into account the volume of complaints it considers
- promote to the public the role of the eSafety Commissioner, including the cyberbullying complaints scheme
- consider improvements to the process by which the eSafety Commissioner can access relevant data from social media services hosted overseas, including account data, that would assist the eSafety Office to apply the end-user notice scheme
- consider whether amendments to the Online Safety Act relating to the eSafety Commissioner and the cyberbullying complaints scheme would be beneficial, and in particular, consider:
    - expanding the cyberbullying complaints scheme to include complaints by adults;
    - expanding the application of the tier scheme by amending the definitions of 'social media service' and 'relevant electronic service', and
    - increasing the basic online safety requirements for social media services.

The Government will consider the report's recommendations and respond in due course.

At the Council of Australian Governments (COAG) meeting on 9 February 2018, COAG agreed that a working group of senior officials from First Ministers', Education, Justice and Health departments consider existing and potential initiatives to help combat bullying and cyberbullying and establish a work program to be led by the Education Council.[7] The Education Council will report to COAG at its next meeting on tangible measures to address any identified need.

About the Online Content Scheme (including past reviews)

In 1999, Schedule 5 to the BSA was introduced (effective 16 July 1999) to extend the co-regulatory system for broadcasting to internet content hosted in Australia and internet carriage services provided to end users in Australia. At its core, the Schedule created a complaints-based 'take-down' regime to require internet content hosts to remove prohibited, or potentially prohibited, online content. In 1999, content was prohibited if it was classified, or would have been classified, Refused Classification (RC) and X-rated (X), or Restricted (R) (unless subject to adult verification mechanisms to prevent access by minors). In 2007, Schedule 7 added MA 15+ content to the definition of 'prohibited content' where such content is made available on a commercial basis online, and not placed behind a restricted access system (RAS).

Past reviews, recommendations and amendments to the BSA highlight how regulators have attempted to keep pace with an ever-evolving communications environment. This current Review of the Online Content Scheme is not intended to revisit the issues identified in past reviews, but rather build on them.

A Review of Schedule 5 in 2002 recommended a new co-regulatory framework for convergent content, provisions for handling ephemeral content such as live streamed audio-visual services, and extension of the existing framework to telephone sex and premium rate services.[8] Convergent content referred to content delivered using 'convergent devices' including mobile phones and other mobile communications devices that could act as multimedia platforms, and, in particular, deliver audio-visual content. Schedule 5 did not cover convergent content.

In 2007, Schedule 7 was introduced (effective 20 January 2008) as a specific regulatory response at that time to changes in technology and to perceived community concern arising from the lack of regulation around emerging media delivery options. The new Schedule largely replicated Schedule 5, to the extent that it regulated internet content hosts, and extended regulation to live streamed content services, mobile phone-based services, and services that provide links to content.

In February 2012, the Australian Law Reform Commission (ALRC) report, *Classification—Content Regulation and Convergent Media* (ALRC Classification report), examined the operation of the National Classification Scheme and Schedule 7 to the BSA. The ALRC identified a range of problems inherent in the classification arrangements and broader regulatory framework, including an inadequate regulatory response to changes in technology and community expectations.[9] The ALRC recommended the establishment of a new classification scheme, administered by a single Commonwealth regulator that covered all media content across all platforms. The Department will be consulting on how to modernise the National Classification Scheme through a separate discussion paper.

In 2012, a Statutory Review of Schedule 7 was conducted as part of the review of Australia's media and communications policy framework (Convergence Review). The Convergence Review concluded there was a continued need for a scheme such as the one created by Schedule 7, but raised issues for its future maintenance, including the inconsistencies created by the Restricted Access Systems Declaration 2007[10] for content regulation across different platforms and media, effective and efficient complaints handling, and how the operational and definitional issues observed in the current scheme could be addressed in the future.[11]

The Convergence Review took into account the views of the ACMA and conclusions of the ALRC Classification Report and agreed in principle with the ALRC that the functions of Schedule 7 form part of a technology-neutral classification scheme for regulating adult content administered by a single Commonwealth regulator. If the recommendations of the ALRC were not accepted or were delayed in implementation, the Convergence Review proposed a range of amendments to Schedule 7 to improve its practical operation.

Oversight of Schedules 5 and 7 was transferred from the ACMA to the eSafety Commissioner under subparagraph 15(1)(a)(ii) of the Online Safety Act on 1 July 2015. It was considered that there were operational efficiencies and synergies in doing so given the eSafety Commissioner's role in administering the Rapid Removal Scheme for cyberbullying content.

Both Schedules 5 and 7 required codes of practice. These codes have not been reviewed since they were established; the three codes relating to Schedule 5 were registered in May 2005 and the code of practice required for Schedule 7—the *Content Services Code*—took effect from 10 July 2008.

Consultation process

The Department is seeking views from stakeholders and interested parties in response to the Terms of Reference and the questions put forward in this discussion paper. The Department welcomes single or consolidated submissions on the Online Safety Act and the Online Content Scheme. Submitters may also if they wish, direct views to specific questions only.

It is expected that follow-up meetings will be conducted with stakeholders that are directly involved in administering the legislation, or would be impacted by any reforms. These meetings are likely to be scheduled during late July and early August 2018, following consideration of written submissions.

How to make a submission

The Department invites submissions by **5.00 pm AEST on Wednesday 25 July 2018**. Submissions may be lodged in the following ways:

Website	www.communications.gov.au/have-your-say
Email	onlinesafety@communications.gov.au
Post	Director, Online Content and eSafety Section Department of Communications and the Arts GPO Box 2154 Canberra ACT 2601

Submissions should include your name, organisation (if relevant) and contact details. The Department will not consider submissions without verifiable contact details.

Submissions will be treated as non-confidential information, and can be made publicly available on the Department's website, unless a respondent specifically requests its submission, or a part of its submission, is kept confidential, and provides acceptable reasons. An email disclaimer asserting confidentiality of the entire submission is not sufficient, nor is a header or footer disclaimer.

The Department reserves the right not to publish a submission, or any part of a submission, at its absolute discretion. The Department will not enter into any correspondence with respondents in relation to any decisions not to publish a submission in whole or in part.

The Department is subject to the *Freedom of Information Act 1982* and may be required to disclose submissions in response to requests made under that Act.

The *Privacy Act 1988* establishes certain principles regarding the collection, use and disclosure of information about individuals. Any personal information respondents provide to the Department through submissions will be used for purposes related to considering issues raised in this paper, in accordance with the Privacy Act. If the Department makes a submission, or part of a submission, publicly available the name of the respondent will be included. Respondents should clearly indicate in their submissions if they do not wish their name to be included in any publication relating to the consultation that the Department may publish.

Questions about the submission process can be directed to onlinesafety@communications.gov.au.

Next steps

The Online Safety Act and the Online Content Scheme Reviews will be conducted concurrently and be undertaken by an independent expert appointed by the Minister for Communications. The independent expert will be supported by staff from the Department.

It is intended that the Reviews will be completed by the end of September 2018 and a report provided to the Minister for Communications.

The final report on the Reviews will be tabled in Parliament. Any recommended changes to the Online Safety Act and the Online Content Scheme will then be considered by the Government.

Review of the Online Safety Act

This section of the discussion paper focuses on the Online Safety Act. The Online Content Scheme is considered in the next section.

The purpose of the Online Safety Act is to enhance the capacity for Australians to engage online in a safe manner, including by protecting Australian children from cyberbullying harm on electronic and social media services.

Why review is required

Section 107 of the Online Safety Act requires that a review of the operation of the Act be initiated within three years after its commencement. The Act commenced on 1 July 2015. This Review satisfies section 107.

The Statutory Review of the Act is important for the Government to ensure that the eSafety Commissioner has the appropriate powers, functions and supporting governance arrangements to deliver on its mandate to enhance online safety for all Australians now and in the future.

Statutory powers and functions of the eSafety Commissioner

The Online Safety Act establishes and sets out the powers and functions of the eSafety Commissioner, an independent statutory office, supported by the ACMA. The functions of the eSafety Commissioner related to online safety listed in section 15 of the Online Safety Act include to:

- promote online safety
- support and encourage the implementation of measures to improve online safety for Australians
- coordinate activities of Commonwealth Departments, authorities and agencies
- collect, analyse, interpret and disseminate information
- support, encourage, conduct, accredit and evaluate educational and promotional and community awareness programs
- make grants
- support, encourage, conduct and evaluate research
- publish reports and papers
- advise and provide reports to the Minister
- consult and cooperate with other persons, organisations and governments
- monitor and promote compliance with the Online Safety Act, and
- formulate guidelines and statements on online safety best practice or guidelines and statements that are directed towards facilitating the timely and appropriate resolution of incidents involving cyberbullying material targeted at an Australian child as well as promote these.

The specific functions conferred on the eSafety Commissioner by clauses 94 of both Schedules 5 and 7 to the BSA, include to:

- monitor compliance with internet and content services industry codes and standards
- advise and assist parents and responsible adults in relation to the supervision and control of children's access to internet content and content services
- conduct and coordinate community education programs about internet content, internet carriage services and content services in consultation with relevant groups and agencies
- conduct and commission research into issues relating to internet content, internet carriage services and content services

- liaise with regulatory and other relevant bodies overseas about cooperative arrangements for the regulation of the internet and commercial content services industries, including but not limited to, collaborative arrangements to develop multilateral codes of practice and content labelling technologies; and
- to inform himself/herself and advise the Minister on technological developments and service trends in the internet and commercial content services industries.

The Online Safety Act also sets out other matters, which are integral to the proper functioning of the Act and implementation of the Government's online safety commitments, including the enforcement mechanisms available to the eSafety Commissioner such as civil penalties, enforceable undertakings and injunctions.

Administration and governance of the eSafety Commissioner

The Online Safety Act also provides for the administration of the eSafety Commissioner. Although the eSafety Commissioner is a statutory officeholder, the Commissioner's office has not been established as an entity as defined in the *Public Governance, and Accountability Act 2013* (PGPA Act). This means that the eSafety Commissioner is not able to exercise accountable authority responsibilities under the PGPA Act.

ACMA administrative support

Under section 67 of the Act, the ACMA must provide assistance as is reasonably required to the eSafety Commissioner to enable the Commissioner to perform functions and exercise powers. This assistance can include, but is not limited to, the provision of advice, administrative resources or facilities and staffing.

Staffing

The ACMA must provide staff to assist the eSafety Commissioner. This means that eSafety Office staff are Australian Public Service (APS) employees of the ACMA. There are no provisions under the Online Safety Act for the eSafety Commissioner to hire staff directly.

Delegation power

In addition, section 63 of the Act limits the eSafety Commissioner's powers to delegate 'any or all' functions to ACMA staff, and only to ACMA staff that are APS employees at a minimum level of APS6. Although the eSafety Commissioner has the power to enter into contract (under section 60 of the Act), and has used this power to engage contractors, the delegation limitation means that contractors are not able to be delegated power to exercise the Commissioner's full functions. This may limit the work that contactors can undertake for the eSafety Commissioner.

Under section 64 of the Act the eSafety Commissioner is able to delegate to a body corporate any or all functions in relation to complaints about cyberbullying material and social media services with the exemption of powers to issue social media notices and formal warnings (under sections 35 and 37 of the Act). This power to outsource the functions of the eSafety Commissioner has not been used. It is similar to provisions in New Zealand's *Harmful Digital Communications Act 2015* which has been used to delegate complaints handling and investigation powers to a non-government agency.

Information handling and disclosure powers

Part 9 of the Online Safety Act sets out rules about how the eSafety Commissioner must handle information obtained in the course of exercising legislative functions. This includes disclosure to the Minister, certain regulatory and law enforcement authorities, school teachers and parents or guardians. Inappropriate disclosure of information could potentially lead to civil or criminal penalties. The eSafety Office has also developed Memoranda of Understanding (MOUs) with law enforcement and educational bodies to set out the procedures for information exchange. The scope of these provisions and the MOUs may not be sufficiently broad to enable the eSafety Commissioner to perform legislative functions and exercise powers under the Online Safety Act, as well as work collaboratively with other parties.

In addition, while the Act provides that it is possible to disclose this information raised in complaints to APS employees, contractors engaged by the Commissioner are not included. Again, this may limit the type of work contractors can do.

Funding

Under current arrangements, the eSafety Commissioner is funded through the Online Safety Special Account (the Special Account) established under Part 8 of the Online Safety Act and administered by the ACMA. Special accounts are used where other types of appropriations are not suitable, including where there is a need for increased transparency where activities are jointly funded. The amount of the ACMA appropriation that is made available to the eSafety Commissioner through the Special Account is determined by the Minister. The 2018–19 Federal Budget committed an additional $14.2 million over four years for the eSafety Commissioner to provide online safety advice and support to all Australians. This is in addition to the $64.8 million allocated for operational and capital funding for the four years commencing from financial year 2018-19.[12]

Reporting

The eSafety Commissioner is required to make an annual report to the Minister for Communications. This report is included in the ACMA's annual report. As the eSafety Commissioner is not subject to the PGPA Act, the Commissioner is not required to prepare a corporate plan (as defined in section 35 of the PGPA Act).

Expanded role of the eSafety Commissioner

The original mandate of the eSafety Commissioner was to enhance online safety for children. In 2017, the Government broadened the general functions of the eSafety Commissioner to cover online safety for all Australians. The expansion of the eSafety Commissioner's functions was, in part, a response to feedback received from Australian adults that they were not aware that the eSafety Commissioner is able to assist all Australians with concerns around illegal or offensive online content, address the issue of sharing of intimate images without consent, and provide general advice about managing technology risks and online safety.

The expansion of functions also acknowledged the expertise of the eSafety Commissioner and the supporting ACMA staff in technology use and abuse, and in developing educational, promotional and community awareness programs on online safety for a wide range of audiences, including families, children, parents, teachers, service providers, and diverse cultural audiences.

From July 2015 to May 2018, the eSafety Commissioner has:

- resolved over 830 complaints about serious cyberbullying that targeted Australian children
- worked with 14 major social media service providers to counter cyberbullying
- referred over 6,940 young people to the Kids Helpline
- conducted over 25,300 investigations into illegal or offensive online content

- received 217 reports related to 349 URLs as well as 110 enquiries between 16 October 2017 and 18 May 2018 regarding the non-consensual sharing of intimate images through its IBA Portal
- certified 35 online safety program providers with over 140 presenters delivering programs in Australian schools
- educated over 227,000 students via Virtual Classrooms and conducted over 105,000 face-to-face presentations, including pre-service teachers, community presentations, teacher professional learning and conferences
- made the iParent portal available to parents, providing advice on a range of online safety and digital content issues;
- launched the eSafety Women site with resources and advice for women, and provided training for more than 5,500 frontline professionals across every state and territory to help women experiencing tech facilitated abuse, and
- launched the Be Connected Portal to provide advice on digital literacy and online safety for seniors (a 2016 election commitment—administered in consultation with the Department of Social Services). (This site has had over 34,000 active users since its launch in October 2017).

Subject to the passage of the Enhancing Online Safety (Non-Consensual Sharing of Intimate Images) Bill 2018,[13] the eSafety Commissioner will also administer a complaints and objections system whereby victims, or a person authorised on behalf of a victim, will be able to lodge a complaint directly to the eSafety Commissioner about an intimate image that has been posted, or threatened to be posted, without consent on a 'social media service', 'relevant electronic service' or 'designated internet service'. Civil remedies can be applied to both the perpetrator and content host, and to social media and content providers who fail to comply with a request to remove offending material. The civil penalty regime will provide a formal reporting and redress system as part of the eSafety Commissioner's IBA Portal.

The eSafety Commissioner was set up as the lead agency to coordinate and lead online safety activities across the Australian Government. Online safety is a complex, emotive and emerging area of public policy where policy measures and support mechanisms are spread across multiple Commonwealth agencies, state and territory governments, law enforcement agencies, industry, non-government organisations and the not-for-profit sector. In addition, schools, educators and parents have a keen interest and a critical role to play. Whilst the need for greater coordination of the work being undertaken by relevant sectors is acknowledged by Government, it is outside the scope of this Review.

Complaints system for cyberbullying material

The eSafety Commissioner administers a cyberbullying complaints system. The Online Safety Act makes it clear that the Government expects all social media services accessible to an Australian child to meet the following three requirements (the Basic Online Safety Requirements):

1. terms of use which sufficiently prohibit cyberbullying material;
2. a complaints scheme under which users can seek to have material which breaches the terms of use removed; and
3. a contact point for the eSafety Commissioner to refer complaints that users consider have not been adequately dealt with.

As far as practicable, the eSafety Commissioner communicates these expectations to social media services. The eSafety Commissioner's complaints system offers a safety net for child victims of cyberbullying, that is available where the social media services' existing complaints system has failed.

A complaint may be made to the eSafety Commissioner when a person has reason to believe cyberbullying material targeted at an Australian child has been, or is being, provided on a social media service or relevant electronic service. The person must demonstrate that they have, in the first instance, made a complaint to the social media service under its existing complaints system and that the service has failed to remove the content within 48 hours.

Cyberbullying material is targeted at an Australian child if a reasonable person would consider it likely:

- that the material was intended to have an effect on a particular Australian child, and
- the material would be likely to have a seriously threatening, seriously intimidating, seriously harassing or seriously humiliating effect on the Australian child.[14]

A social media service is defined as an electronic service where the:

- sole or primary purpose of the service is to enable online social interaction between two or more end-users
- service allows end-users to link to, or interact with, some or all of the other end-users, and
- service allows end-users to post material on the service.[15]

The Online Safety Act includes a number of definitions, such as social media service and electronic service, that may need to be reviewed in the context of new technologies (including massive multiplayer online gaming, drones and augmented reality).

In 2016–17, the eSafety Office received 305 complaints about serious cyberbullying, up 63 per cent from the previous year.[16] The primary targets of reported cyberbullying material were Australians aged between 12 and 16 years; 16 per cent of complaints related to children 11 years and under.[17] Cyberbullying covers a wide range of behaviours. Most complaints fell into the general categories of nasty comments and/or serious name-calling (around 68 per cent), threats of violence (around 27 per cent), and offensive or upsetting pictures or videos (around 21 per cent). Complaints were also received in relation to fake and/or impersonator accounts (around 18 per cent), unwanted contact (around 13 per cent) and sexting/revenge porn (around 12 per cent).[18] A complaint may relate to more than one category.

The eSafety Commissioner has the power to investigate complaints and conduct such investigations as the Commissioner sees fit. As cyberbullying and other content may be very distressing, the eSafety Commissioner provides support for victims through referral to mental health services. For example, the eSafety Office has a referral agreement with Kids Helpline and since 2015 has referred over 6,940 young people.

Rapid Removal Scheme

Part 4 of the Online Safety Act sets out a two-tiered scheme for the rapid removal of cyberbullying material targeted at an Australian child from large social media services (the Rapid Removal Scheme). The Rapid Removal Scheme has been successful, with the eSafety Commissioner working in collaboration with social media partners to have cyberbullying material quickly removed, often in less than a day. To date over 830 complaints have been made to the eSafety Commissioner by children or parents seeking removal of cyberbullying material. The voluntary removal of cyberbullying material by social media companies has been achieved in every case.

Large social media services under tier 1 participate in the scheme on a cooperative basis. Following investigation of a complaint, the eSafety Commissioner may request that the tier 1 social media service remove the cyberbullying material, but there is no legal obligation on the social media service to comply. Social media services can apply to be declared by the Minister as tier 1 services. The Tier 1

social media services are airG, Ask.fm, Flickr, musical.y, Roblox, Snapchat, Twitter, Yahoo!7 Answers, Yahoo!7 Groups, and Yubo.

If a tier 1 large social media service repeatedly fails to remove cyberbullying material following requests from the eSafety Commissioner over a period of 12 months, the eSafety Commissioner has the power to recommend to the Minister for Communications that the service be declared a tier 2 social media service.

A tier 2 social media service is legally required to comply with a notice issued by the eSafety Commissioner to remove cyberbullying material, or face civil penalties. The Tier 2 social media services are Facebook, Google+, Instagram and YouTube.

The Rapid Removal Scheme is intended to be light-touch regulation. It aims to minimise the impact on the social media service industry by utilising existing complaints handling processes and online safety initiatives, whilst still offering tangible and meaningful benefits for children who are victims of cyberbullying, their parents and teachers.

The eSafety Commissioner works collaboratively with key social media services to tackle cyberbullying. While the eSafety Commissioner does not have the authority to compel sites and services hosted overseas (that are not social media partners with the Commissioner under the two-tiered scheme) to remove content, many of these sites and services remove content at the eSafety Commissioner's request on a voluntary basis. The eSafety Commissioner continues to engage with industry, including smaller app developers individually, in a bid to get more services formally into the two-tiered scheme.

End-user Notice Scheme

Part 5 of the Online Safety Act sets out the cyberbullying remediation notice regime (the End-user Notice Regime). Under the regime, the eSafety Commissioner has the power to issue a notice against a particular end-user who posts cyberbullying material targeted at an Australian child, requiring the end-user 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. If the end-user does not comply, the eSafety Commissioner can issue a formal warning or obtain an injunction.

The regime applies to material that is transferred, sent, posted, published, disseminated or otherwise communicated by means of an electronic communication on social media sites, email, text messages, online games and chat functions on websites.

To date, the eSafety Commissioner has not issued an End-user Notice. The eSafety Commissioner has worked closely and collaboratively with the social media services to rapidly remove cyberbullying material while referring children and young people to dedicated support services, including counselling. The success of this informal approach has meant that the eSafety Commissioner has not had to exercise formal powers under Part 5 of the Act.

Questions

Key questions to guide this Review are listed below:

1 Functions and powers of the eSafety Commissioner

Question 1(a): *Are the current functions and powers in the Online Safety Act sufficient to allow the eSafety Commissioner to deliver on the role's mandate? If not, what additional functions could make the eSafety Commissioner more effective? Are there any of the current functions that could be removed?*

Question 1(b): *Are the rules about information handling and disclosure too restrictive considering that the eSafety Commissioner's functions include consulting and cooperating with bodies that may not be specified as permitted disclosees?*

Question 1(c): *Schedules 5 and 7 of the BSA (Online Content Scheme) provide additional functions for the eSafety Commissioner. Is there any merit in moving the Commissioner's Online Content Scheme functions into the Online Safety Act so that all of the eSafety Commissioner's functions and powers are in the same legislation?*

Question 1(d): *Does the way the eSafety Commissioner's functions and powers are specified create barriers preventing, or limiting, the Commissioner from enhancing online safety for Australians or that may prevent, or limit, the Commissioner from responding to new risks in the future?*

2 Administration of the eSafety Commissioner

Question 2(a): *Do the administrative and other provisions in the Online Safety Act provide an appropriate governance structure for the eSafety Commissioner?*

Question 2(b): *Is the ACMA still best placed to provide administrative support to the eSafety Commissioner?*

Question 2(c): *Should the Online Safety Act be amended to give the eSafety Commissioner more independence, particularly in relation to resourcing (including staffing) and funding? If so, is there other legislation that provides an appropriate model?*

Question 2(d): *Does the eSafety Commissioner require a broader delegation power? If so, how would it be limited?*

Question 2(e): *Should the eSafety Commissioner consider delegating some or all functions to a body corporate?*

Question 2(f): *The eSafety Commissioner is not an entity or accountable authority under the PGPA Act or an agency head under the Public Service Act. Is this still appropriate?*

3 Effectiveness of the eSafety Commissioner

Question 3(a): *Has the eSafety Commissioner been effective in enhancing online safety for Australian children since its establishment in 2015?*

Question 3(b): *The scope of the Online Safety Act was expanded in 2017 to cover all Australians. Has it been effective in relation to groups other than children?*

4 Regulatory approach

Question 4(a): *Is the balance right between government intervention and other measures (e.g. developing an individual's ability to identify, assess and self-manage risks) to address online safety in Australia?*

Question 4(b): *The Online Safety Act does not have an express statement about regulatory approach. This is common in other Acts such as the Broadcasting Services Act 1992. Does the Online Safety Act need a regulatory approach statement?*

5 Cyberbullying complaints system

Question 5(a): *Are the Basic Online Safety Requirements in section 21 of the Online Safety Act appropriate? Should they apply to a broader range of platforms or include additional requirements?*

Question 5(b): *Has the Cyberbullying Complaints Scheme, including the Rapid Removal Scheme and End-user Notice Regime, been successful in protecting Australian children from the harm caused by cyberbullying material on large social media sites?*

Question 5(c): *The eSafety Commissioner has not needed to use statutory powers under the Rapid Removal Scheme or the End-User Notice Scheme but has had material removed through industry cooperation. Is an industry-based approach (e.g. codes or other self-regulation) the preferred approach?*

Question 5(d): *Does the End-User Notice Scheme provide an appropriate safety net if industry cooperation fails?*

Question 5(e): *Is the current definition of cyberbullying in paragraph 5(1)(b) of the Online Safety Act general enough to capture the main sources of cyberbullying material causing harm to Australian children?*

Question 5(f): *Considering that there is a COAG Education Council work program on cyberbullying, should the definition of cyberbullying be de-coupled from the Online Safety Act (or expressed more broadly) to ensure that it can evolve as community attitudes change?*

Question 5(g): *Should the cyberbullying complaints system be expanded to cover other types of harmful content not already covered? If so, what types of content should be covered?*

Question 5(h): *The cyberbullying scheme applies to two tiers of social media services. The power to declare a social media service as a Tier 2 service is reserved to the Minister for Communications. Is this appropriate or should the eSafety Commissioner be given this power?*

Question 5(i): *Is the tiered system still the best approach? If not, are there other approaches that would be preferable?*

Review of the Online Content Scheme

The Online Content Scheme is a co-regulatory scheme aimed at addressing community concerns about illegal and offensive online content, and protecting children from exposure to inappropriate material. It is established by Schedules 5 and 7 to the BSA.

The Schedules set out the complaints-based mechanism for 'prohibited content' and 'potential prohibited content' based on the classification categories in the National Classification Scheme. Schedule 5 is concerned with internet service providers (ISPs) restricting access to content hosted overseas where the content provider is outside the Australian jurisdiction. Schedule 7 deals with 'hosting service providers', 'live content service providers' and 'links service providers' (collectively defined as 'designated content/hosting service providers') that provide access to material from within Australia, for example, via a website, webcam or a link on a webpage. Both ISPs and content/hosting service providers have obligations and constraints placed upon them by industry codes which are registered and monitored by the eSafety Commissioner.

The scheme is also supported by non-legislative measures such as community education and international cooperation. The eSafety Commissioner has a role in educating and informing end-users about managing access to prohibited content on the internet, including providing advice to parents on setting up parental controls, installing filtering software and using safe search techniques. Industry codes also endorse and support end-user empowerment by encouraging the provision of information to end-users about content issues and online safety, end-users' rights online, and the development of effective strategies for managing children's use of the internet.

The eSafety Commissioner is required by clause 69 of Schedule 7 to report prohibited content or potential prohibited content to a law enforcement agency if the Commissioner is satisfied that the content is of a sufficiently serious nature to warrant referral to a law enforcement agency. The Commissioner works closely with Australian policing agencies (including federal, state and territory) to combat the most serious criminal online content, such as child sexual abuse material (CSAM) and pro-terror content. MOUs govern the referral processes to ensure the most efficient exchange of pertinent operational information between the eSafety Commissioner and specialist police child exploitation units.

The eSafety Commissioner also liaises with regulatory and other bodies overseas about cooperative arrangements for the regulation of the internet and commercial content labelling technologies and is a member of the International Association of Internet Hotlines (INHOPE) which is a global network of 51 hotlines worldwide dedicated to eradicating CSAM from the internet.

The eSafety Commissioner's specific powers under the Online Content Scheme as well as the Online Safety Act complement other Australian laws that can apply to online behaviour and content. For example, anti-discrimination laws may be applied to online content that constitutes sexual harassment or racial vilification. There are also specific offences under the *Commonwealth Criminal Code Act 1995* (Criminal Code), which make it a crime to use the internet or phone in a menacing, harassing or offensive way or to use the internet or phone to threaten to kill or cause serious harm to another person. In 2005, the Government also made it an offence to use a carriage service to access, transmit or otherwise make available suicide-related material, and possession, production, supplying or obtaining suicide-related material for use through a carriage service.

Section 474.25 of the Criminal Code requires an ISP or content host to refer details of child abuse material to the Australian Federal Police (AFP), where it becomes aware that the service can be used to access that material. This provision does not require ISPs and content hosts to monitor their services for child abuse material, but rather ensures that material is referred for law enforcement consideration when the service provider becomes aware of the existence of the material.

Section 313 of the *Telecommunications Act 1997* provides Australian agencies, including state government agencies, with the ability to obtain assistance from the telecommunications industry when upholding Australian laws. The AFP has responsibility for website blocking requests under section 313. The AFP uses section 313 to disrupt illegal online activity where other mechanisms have been or are likely to be unsuccessful.

Through the Access Limitation Scheme, the AFP predominantly uses section 313(3) requests to block access to INTERPOL's 'Worst of List' of child exploitation websites. When an Australian user attempts to access a website contained on the Worst of List, they are redirected to an INTERPOL 'stop page', blocking access to information containing child abuse material. The AFP provides the list to Australian ISPs, and relies on them to block the identified websites in Australia.

While relevant, consideration of these other laws is outside the scope of this Review.

Why review is required

The explosion of user-generated content and over-the-top (OTT) applications, including social media services, has made regulating what Australians, particularly children, see online extremely challenging and has put pressure on the regulatory framework.

A major concern for parents (and the community) is the increasing accessibility of online pornography and the harm it may cause to children who are exposed to it. While adult websites continue to be an avenue for children to access pornography, sexualised content is increasingly embedded in sites that allow user-generated content such as blogs, photo-sharing or video-sharing websites and social media sites.

Other kinds of harmful content, such as videos containing extreme violence such as beheadings, content inciting suicide or hate crimes, and terrorist-related material, which is prohibited or potential prohibited content under the Online Content Scheme, is widespread on user-generated content sites. User-generated content may be shared within the private features of a social networking service—known as 'dark social' or 'hidden social'—or streamed to many through live features, it may only be transitory and remain online for only brief periods of time, or be rapidly moved from site to site, making it extremely difficult to regulate what is shared between users.

The most concerning content online is CSAM. Developments in anonymous and encrypted networking and new hosting arrangements are increasing opportunities for such content to be distributed, and making it more difficult to determine where it is hosted. By obscuring hosting location, take-down is frustrated and the investigation and apprehension by law enforcement of those who propagate CSAM made more challenging.

Schedules 5 and 7 to the BSA, and the four industry codes made under them, were developed in a pre-smartphone/pre-social media world and may not reflect the reality of the online experiences, digital technologies and consumption of content by Australian consumers today. Industry has been calling for a review of the Online Content Scheme as they are unable to comply with many aspects of the legislation and codes. The eSafety Commissioner has also highlighted that the current framework is misaligned with current technologies, usage patterns, community concerns and enforcement mechanisms, especially in relation to some of the most concerning content.

Australia needs a flexible framework for regulating online content that can adapt to new services and platforms and changing consumer behaviour, and reflects contemporary community standards and expectations. The framework needs to be a streamlined one that provides certainty for industry and regulators.

The current Review will examine the relevance and effectiveness of the Online Content Scheme in today's communications environment and consider how the regulatory framework could be modernised and streamlined. It will also examine the scope of the scheme and what kinds of content should be covered, as well as other approaches for regulating online content, including the 'best of breed' international models. Once the Review is completed, and depending on the recommendations made, the Government may also consider how schemes for regulating online content fit within the broader media and communications framework.

Complaints system for 'prohibited' and 'potential prohibited' content

Any person who is an Australian resident or a company carrying on a business in Australia can complain to the eSafety Commissioner about 'prohibited' or 'potential prohibited' content online, or the hosting of, or linking to, such content. The eSafety Commissioner provides a hotline as well as an online complaints form. The eSafety Commissioner's practice is to investigate all valid complaints. In addition, the Commissioner may choose to investigate a matter on the Commissioner's own initiative.

Link to National Classification Scheme

Prohibited content includes content that has been classified by the Classification Board using the National Classification Code and classification guidelines as:

- *Refused Classification (RC)*—includes CSAM, material that advocates the doing of a terrorist act, detailed instruction or promotion in crime or violence, instruction in paedophilic activity, and gratuitous, exploitative and offensive depictions of violence or sexual violence
- *X 18+*—content that contains explicit sexual activity between adults
- *R 18+ unless it is placed behind a restricted access system*—content that is of high impact and includes violence, drug use, nudity or realistically simulated sex.
- *MA 15+ and is provided on a commercial basis, unless it is placed behind a restricted access system*—content that is strong impact.

Potential prohibited content is content that is likely to be classified in one of the above 'prohibited' categories, if it were to be classified.

The Restricted Access Systems Declaration 2014 (the RAS declaration)[19] requires that all Australian-hosted R 18+ content, and some MA 15+ content be provided subject to an RAS, which is a basic means of 'age-gating' content.

Complaints statistics indicate that mainstream community concerns are predominately related to the eradication and prevention of CSAM. Around 80 per cent of items actioned by the eSafety Commissioner in 2016–17 related to RC content, with the vast bulk dealing with CSAM.[20] This suggests that the scope of content that is captured by Schedules 5 and 7 might not reflect community expectations of what should be prohibited.

During 2016–17, the eSafety Commissioner identified 7075 items of prohibited and potential prohibited content; all of these items were hosted overseas and were referred by the eSafety Commissioner to the makers of optional end-user internet software filters under Schedule 5 and the registered code of practice.[21] No final take-down notices were issued to Australian content hosts during this period.[22]

In order for the eSafety Commissioner to issue a final notice to take down internet content hosted in Australia, the content must be classified by the Classification Board as prohibited content.

The Department will be consulting on how to modernise the National Classification Scheme through a separate discussion paper.

Content location

The process for dealing with prohibited and potential prohibited content depends on the content's location (i.e. where it is hosted):

- if content is hosted outside Australia—in the course of an investigation under Schedule 7, the eSafety Commissioner can notify the content to industry under:
  - the 'designated notification scheme' set out in the industry code registered under Schedule 5 to allow content to be filtered; or
  - issue a 'standard access-prevention notice' under Schedule 5 directing an ISP to take all reasonable steps to prevent end-users from accessing the content, and
- if content is hosted in Australia, the eSafety Commissioner can issue a 'take-down', 'service-cessation' and 'link-deletion' notice under Schedule 7 as appropriate to remove content or end the service.

Sanctions

These prohibitions are backed by strong sanctions for non-compliance, including criminal penalties for serious offences.

Referral to law enforcement

There is a complementary process for content that the eSafety Commissioner considers 'sufficiently serious', such as CSAM; material that promotes, incites or instructs in matters of crime or violence; or material that advocates the doing of a terrorist act:

- if the content is hosted in Australia—the eSafety Commissioner can refer the content to domestic police services, and
- if the content is hosted outside Australia—the eSafety Commissioner can refer the content to the AFP, Interpol and/or INHOPE.

Industry codes of practice

Schedules 5 and 7 establish a co-regulatory model based on the existence of codes of practice developed by the internet and content services industry. Schedule 5 specifies matters to be dealt with in an internet industry code and Schedule 7 specifies matters to be dealt with in a content services code.

Four industry codes are registered under Schedules 5 and 7.[23] The Communications Alliance is the industry body responsible for these codes. There are three codes registered under Schedule 5 for internet and mobile content—*Code 1: Hosting Content within Australia Code*, *Code 2: Providing Access to Content Hosted within Australia Code, Code 3: Providing Access to Content Hosted outside Australia Code* and a fourth code, registered under Schedule 7, for internet content—the *Content Services Code*.

The codes impose various obligations on ISPs, mobile carriers and content service providers, including in relation to:

- responding to notices from the eSafety Commissioner
- information to be provided by ISPs to content providers and end-users
- making Family Friendly Filters (FFF) available

- establishing complaints procedures;
- 'opt-in' requirements for restricted content on mobiles
- assessment and classification of content, and
- use of restricted access systems (RASs).

Compliance with an industry code is voluntary unless the eSafety Commissioner directs a particular participant in the internet industry to comply with the code. The eSafety Commissioner may create an industry standard where the codes are either not working or non-existent. Compliance with an industry standard is mandatory. Complaints may be made to the eSafety Commissioner under the Online Content Scheme about a breach of an industry code or standard.

Questions

6 Online content complaints system

Question 6(a): *The Online Content Scheme was enacted at different times in two separate schedules to the BSA. Is there clarity about the scope of each schedule?*

Question 6(b): *Is the Online Content Scheme effective in limiting the availability of prohibited content?*

Question 6(c): *Is the Online Content Scheme providing an adequate safeguard for Australian children?*

Question 6(d): *Does the Online Content Scheme give the eSafety Commissioner appropriate powers to investigate and resolve complaints?*

7 Online content enforcement mechanisms

Question 7(a): *Are the enforcement tools available to the eSafety Commissioner appropriate?*

Question 7(b): *Do the 'take-down', 'service-cessation' and 'link-deletion' notices provided by Schedule 7 to the BSA ensure that, once detected, prohibited content is removed quickly and effectively?*

Question 7(c): *Is the 'take-down' notice provided by Schedule 5 to the BSA effective, particularly in relation to content hosted outside of Australia?*

8 Link with the National Classification Scheme

Question 8(a): *Is reliance on the National Classification Scheme categories to identify prohibited and potential prohibited content appropriate and sufficiently flexible to respond to the types of content that may emerge in the online environment?*

Question 8(b)*: Is it appropriate that content must be classified by or referred to the Classification Board for a take-down notice to be issued?*

9 Regulatory framework

Question 9(a): *Should Schedules 5 and 7 be repealed and a new combined scheme for regulating prohibited content created? If so, should any new scheme remain in the Broadcasting Services Act?*

Question 9(b): *Should the current regulatory framework be replaced by a technology-neutral scheme that captures newer platforms and services? If so, how could a new scheme address the definitional and operational issues identified in the current scheme?*

Question 9(c): *Are there any other options for regulating online content, including overseas models, which could work in Australia? If so, what are the advantages and disadvantages of such models?*

10 Industry codes

Question 10(a): *Is the co-regulatory approach (that is, based on the four industry codes) operating as it should? Do the codes provide adequate safeguards without imposing unnecessary financial and administrative burdens on the internet and content services industry?*

Question 10(b): *The industry codes were made in 2005 and 2008. Have the Codes kept pace with changes in technology and consumer behaviour?*

Question 10(c): *Have the industry codes encouraged the development of internet technologies and their application?*

Question 10(d): *There are four separate codes, found in two separate documents. Would a combined, single code provide clarity and be easier to administer and enforce?*

Question 10(e): *Do the industry codes reflect current community attitudes?*

Question 10(f): *Is the Family Friendly Filter (FFF) scheme effective in protecting Australian families from prohibited content?*

Question 10(g): *Are there any other commercial content filtering or automated content monitoring solutions (such as algorithms) that can help to protect Australian families? What options are there for identifying harmful or prohibited content?*

Question 10(h): *Is prohibited content a subject that is better dealt with in an industry standard or determination than in legislation?*

11 Other issues

Question 11: *Please provide any additional comments about the Online Safety Act or the Online Content Scheme that have not been covered in your answers to other questions in this discussion paper.*

Endnotes

1 *Enhancing Online Safety Act 2015* (Cth).
2 *Broadcasting Services Act 1992* (Cth) Schedules 5 and 7.
3 *Enhancing Online Safety (Family and Domestic Violence) Legislative Rules 2015*. The eSafety Women program helps empower vulnerable women through training of frontline workers who deal with women facing technology-facilitate abuse and providing a range of resources on the eSafety Women website designed to help women manage technology risks and abuse by giving them the tools they need to be confident online.
4 Explanatory memorandum to the Enhancing Online Safety for Children Amendment Bill 2017.
5 Senate Environment and Communications References Committee *Harm being done to Australian children through access to pornography on the internet* (2016).
6 Senate Legal and Constitutional Affairs References Committee *Adequacy of existing offences in the Commonwealth Criminal Code and of state and territory criminal laws to capture cyberbullying report* (2018).
7 COAG meeting Communiqué, 9 February 2018.
8 *Report of the Review of the Operation of Schedule 5 to the Broadcasting Services Act 1992* (2004), Issue 133.
9 ALRC *Classification – Content Regulation and Convergent Media* (2012), Report 118.
10 The Declaration provided that MA15+ and R18+ content be subject to a RAS.
11 Department of Broadband, Communications and the Digital Economy *Convergence Review Final Report* (2012), Appendix G: Report on review of Schedule 7 of the Broadcasting Services Act.
12 Calculated on basis of funds included in Table 2.1.1 for Program 1.3 less additional $14.2 million budget allocation: *Portfolio Budget Statements 2018-19, Budget related Paper No. 1.3: Communications and the Arts Portfolio*, page 95, www.communications.gov.au/who-we-are/department/budget/2018-19-budget-communications-and-arts-portfolio.
13 Enhancing Online Safety (Non-consensual Sharing of Intimate Images) Bill 2018.
14 Section 5 of the *Enhancing Online Safety Act 2015* (Cth).
15 Section 9 of the *Enhancing Online Safety Act 2015* (Cth).
16 Office of the eSafety Commissioner, Annual Report 2016–17, p 115.
17 Ibid, p116.
18 Ibid, p117.
19 *Restricted Access Systems Declaration 2014*.
20 Ibid, p119.
21 Ibid, p118.
22 Ibid, p118.
23 Internet Industry Codes of Practice (Content Code 1: Hosting content within Australia, Content Code 2: Providing access to content hosted within Australia and Content Code 3: Providing access to content hosted outside Australia) and Content Services Code.