Australian Government

Office of the
eSafety Commissioner

AUGUST 1, 2018

SUBMISSION

REVIEWS OF THE ENHANCING ONLINE SAFETY ACT 2015 AND THE ONLINE CONTENT SCHEME

JULIE INMAN GRANT
OFFICE OF THE ESAFETY COMMISSIONER

FOREWORD ***4***
PART 1 ***5***
Introduction ***5***
Structure **5**
Regulatory approach **5**
Cyberbullying reporting scheme **7**
Cyber abuse **8**
CyberReport tool for illegal content **8**
Image-based abuse portal and reporting tool **9**
Research **10**
Resources **11**
Be Connected **13**
eSafetyWomen **14**
Women Influencing Technology Spaces **15**
Voluntary certification scheme for online safety program providers **15**
Stakeholder engagement **15**
Prevention through Safety-by-Design **17**
Media and communications **17**
Conclusion ***18***
PART 2 ***19***
Question 1(a) and 1(d): ***19***
Question 1(b): ***21***
Question 2(a): ***24***
Question 2(b): ***26***
Question 2(c): ***27***
Question 2(d): ***29***
Question 2(e): ***29***
Question 2(f): ***31***
Question 3(a): ***32***
Question 3(b): ***38***
Question 4(a): ***41***
Question 4(b): ***42***
Question 5(a): ***43***
Question 5(b): ***44***
Question 5(c): ***46***
Question 5(d): ***48***
Question 5(e): ***49***

Question 5(f): ***50***
Question 5(g): ***51***
Question 5(h): ***52***
Question 5(i): ***53***
Question 6(a): ***53***
Question 6(b): ***54***
Question 6(c): ***55***
Question 6(d): ***56***
Question 7(a): ***57***
Question 7(b): ***57***
Question 7(c): ***57***
Question 8(a): ***58***
Question 8(b): ***59***
Questions 9(a) and 1(c) ***60***
Question 9(b): ***61***
Question 9(c): ***62***
Questions 10(a), (b), (c), (d), (e) and (f): ***63***
Question 11 ***64***

FOREWORD

The online world is rich with opportunities unforeseen generations ago.

Social media, in particular, has become a powerful tool for Australians of all ages to engage, connect, communicate, learn and grow.

However, the online world is not without risk or harms. Further, online issues are only becoming more complex, pervasive and challenging.

This underscores the importance of the Office of the eSafety Commissioner's (eSafety) role in leading, coordinating and advising on online safety issues to ensure all Australians have safe, positive and empowering experiences online.

As Australia's eSafety Commissioner, I therefore welcome the opportunity to review the online safety regulatory framework to ensure eSafety continues to meet its regulatory objectives.

Part one of this submission provides an overview of eSafety's key functions, activities, structure and achievements.

Part two of this submission specifically responds to the questions in the discussion paper. In particular, we have identified ways of enabling eSafety to perform our functions and activities more effectively and efficiently.

Building upon the work of my predecessors, I am proud of what my office has achieved in just three years. I believe that by adopting the changes to our regulatory framework outlined in this submission, eSafety will have the independence, authority, accountability and clarity it needs to deliver the comprehensive, compassionate and citizen focused services Australians both deserve and demand.

I am committed to leading eSafety, as it continues creating a better online world for all Australians.

PART 1

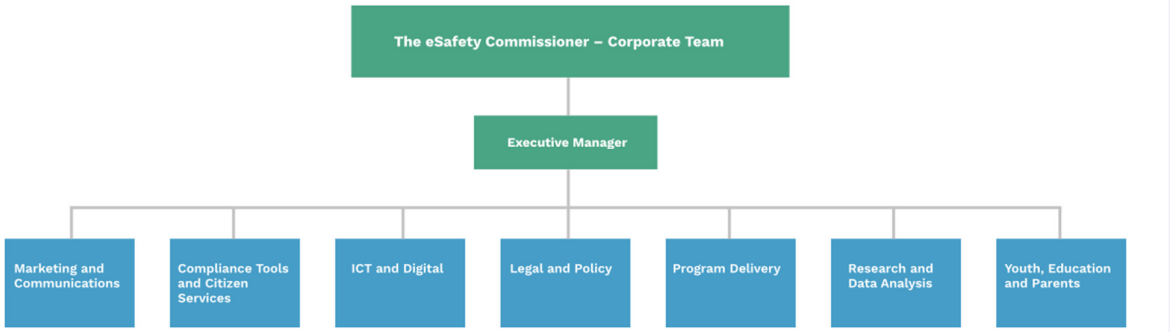
Introduction

The Office of the eSafety Commissioner ('eSafety') was established in July 2015, under the *Enhancing Online Safety Act 2015* (Cth) ('the Act'). The Commissioner's remit was to enhance the online safety of children and young people, primarily through a complaints service for young Australians experiencing serious cyberbullying.

In July 2017, eSafety's remit was expanded to include promoting online safety for all Australians. This broad remit complements s.15 of the Act, which outlines a broad list of functions that together enable the Commissioner to lead, coordinate and advise on online safety issues to ensure all Australians have safe, positive and empowering experiences online.

Structure

eSafety's structure, comprised of seven subject matter teams and the Commissioner's Corporate Team, is designed to correspond with and support the Commissioner's broad remit.[1]



Each team operates pursuant to a team vision, which is designed to correspond with and support eSafety's mission of keeping Australians safer online.

Regulatory approach

eSafety's broad remit requires us to understand and address issues from multiple and reinforcing angles. We therefore adopt a wide, proactive and whole of community preventive approach, which allows us to deliver comprehensive, compassionate and citizen focused services.

The four pillars underpinning eSafety's regulatory approach are *Prevention*, *Protection*, *Partnerships* and *Promotion*.

This underscores the interconnected and multifaceted nature of eSafety's regulatory approach, which begins with prevention and awareness raising and ultimately extends to

[1] A second executive manager for eSafety was approved in July 2018.

our investigative and enforcement regulatory powers, including collaboration with law enforcement agencies.

eSafety's interconnected and multifaceted regulatory approach is also why its three complaints and reporting schemes, outlined below, function as one Investigative Division.

- The Cyber Bullying Complaints Scheme, which investigates serious cyberbullying material targeting an Australian child
- The Online Content Scheme, which investigates offensive and illegal online content, prioritising child sexual abuse material, and
- The Image-Based Abuse Portal, which investigates reports of image-based abuse.

Protecting citizens online requires more than a reliance on investigative and enforcement measures, but rather a proactive approach to addressing complex societal situations and behaviours. While operationally separate, functionally the complaints and reporting schemes act as a singular Investigative Division. This allows the teams to collaborate and refer complaints between the schemes, in order to ensure the best outcome for the complainant.

Depending on the scheme, eSafety can formally or informally request removal of material. While taking down content is one of our main priorities, eSafety's case management approach means we also focus on preventing the behaviours that underpin cyberbullying, as well as supporting and building the resilience of victims.

For example, if a complaint involving a child is of a serious nature, eSafety would not only collaborate with law enforcement, but would consider engaging with parents, carers and education practitioners to provide the interventions, resources and support that children need to understand, manage and resolve online issues. This approach empowers children who have experienced online abuse to take control of their experience and helps reduce the potential for revictimisation.

The following case study illustrates how the intersection between investigative tools, educational materials and early intervention can create a positive online environment for all users.

Case Study

eSafety received three similar cyberbullying complaints, in three days, from complainants in a similar geographic area. The complaints all reported apparent 'hacking issues', which the social media company had not acted upon within 48 hours. Quickly identifying the similar nature of the reports, the cyberbullying investigator communicated with the complainants and their parents and was able to determine their relationship to each other and that all three had made a police report.

By adopting a case management approach to each complaint, but a coordinated approach to the issue overall, the investigator determined the complainants' accounts were not being hacked, but rather manipulated to give up confidential information, specifically 'high value' content (naked images) that they had stored on their accounts. They were threatened that if they didn't provide their passcodes for access, the naked images that had allegedly already been obtained would be shared with their family and friends.

Working with the social media site, the investigator was able to disable the three accounts, speak with the parents and refer the complainants to the Kids Helpline Counselling service.

When it was established other friends of the complainants had also been targeted, eSafety warned the respective schools of the nature of the complaints. The eSafety Education Manager also spoke directly with the three deputy principals. Over the course of 24 hours, the investigative and education teams worked together to provide the schools with an advice document that was shared with their parent and carer communities. This guidance reached over 6,000 parents and carers. The eSafety Education Manager also informed the Police Youth Liaison Officer who offered to follow up with the school communities. eSafety sent this guidance out through multiple vectors, including social media, to keep the broader public aware of the issues.

In a very short timeframe, the school and wider community was able to provide tailored and specific support to the affected students and their schools to both manage their wellbeing and security, while improving their understanding of both the risks and key issues.

By using its expertise and connections with the education community, law enforcement and communications, eSafety not only helped address the particular situation, but helped educate and empower communities to prevent similar situations occurring.

Cyberbullying reporting scheme

As discussed above, one of eSafety's key functions is the Cyberbullying Complaints Scheme, which provides a complaints mechanism for Australian children who experience cyberbullying. Cyberbullying involves the use of technology to seriously harass, intimidate, humiliate or threaten a person. These technologies include social networks, instant messaging and email.

The scheme serves as a safety net for young people who haven't been able to resolve their online issue via the social network's reporting functions. eSafety works closely with social media services to help remove harmful material and provide relief for a young person and their family. Since the introduction of the scheme, we have received over 900 complaints about cyberbullying affecting Australian children.

Tier scheme social media partners

The Act provides a two-tiered scheme for the fast removal from social media services of cyberbullying material targeted at an Australian child. While social media services work with eSafety on a cooperative basis to remove serious cyberbullying material targeted at a child, the two tiers of the scheme are subject to different levels of regulatory oversight.

Tiers 1 and 2

Tier 1 social media services participate in the scheme on a voluntary basis. There are a wide range of services, including Snapchat and Twitter. The Act enables the Minister to declare a social media service to be a Tier 2 service, following a recommendation from the Minister. The current Tier 2 services are Facebook, Google+, Instagram and YouTube.

These services are subject to a civil enforcement scheme that can attract legally binding notices and penalties, including fines of up to $21,000 a day for Tier 2 social media sites that do not comply with take down notices. Under the end-user notice scheme, the Commissioner has the power to give a notice to a person posting the cyberbullying material (the end-user) to remove the material, refrain from posting material which targets the complainant, or to apologise.

While these powers and penalties are available to the Commissioner, eSafety prefers to adopt a cooperative approach to resolving cyberbullying complaints. eSafety has built strong working relationships with the major social media services, which has contributed to a 100% compliance rate for removing offending content from their platforms upon request. By focusing on early intervention to minimise the impact of cyberbullying material, in almost all instances we have been able to have offending content removed within a matter of hours.

Referrals to key support services

eSafety's case management approach to complaints means we focus on preventing the behaviours, attitudes and beliefs that underpin cyberbullying.

eSafety works with parents, carers, schools, communities and law enforcement to address cyberbullying behaviour and refer young people in need of mental health support to services such as Kids Helpline, Parents Helpline and eHeadspace.

This ultimately empowers Australians to build their safety, skills, wellbeing and resilience online.

Cyber abuse

With our expanded remit, eSafety now receives requests for general guidance and support from adults experiencing cyber abuse. The majority of complaints received are from women, mainly in relation to cyberbullying behaviours on the same social media platforms that are reported by children. Since July 2017, eSafety has received over 300 adult cyber abuse reports.

While eSafety has no formal investigative powers in relation to adult cyber abuse, we draw upon our cooperative arrangements with social media services to have serious material removed. We also provide victims with guidance, assistance and referrals to support services for assistance.

More recently, eSafety has developed capacity building programs as part of its commitment to a wide, proactive and multi-angular preventive approach. For example, one of eSafety's newest initiative, Women Influencing Technology Spaces (WITS), not only provides women with information for reporting and addressing cyber abuse, but empowers them with skills and strategies to build their capacity to interact online with impact, confidence and resilience.

CyberReport tool for illegal content

The Online Content Scheme established under Schedules 5 and 7 of the Broadcasting Services Act ('BSA') regulates offensive and illegal online content. The CyberReport Team investigates these reports and acts on material found to be 'prohibited or potentially prohibited', including:

- offensive depictions of children, such as child sexual abuse content
- content advocating terrorism

- instruction, incitement or promotion of crime or violence, and
- sexually explicit content.

The team prioritises reports concerning online child sexual abuse material (CSAM), and works closely with law enforcement and other bodies domestically and internationally to achieve rapid takedown of material around the world.

eSafety's responsibilities under the Online Content Scheme include:

- investigating complaints made under Schedules 5 and 7 to the BSA
- directing take-down of prohibited content if it is hosted in Australia
- notifying all potentially illegal Australian-hosted content to law enforcement
- notifying all overseas-hosted child sexual abuse material to the Australian Federal Police (AFP) or International Association of Internet Hotlines (INHOPE), for rapid police action and take-down in the host country, and
- notifying prohibited URLs to vendors of optional end-user filters.

eSafety is an integral member of INHOPE, which currently comprises 48 hotlines from around the world, and plays a vital role in coordinating global efforts to eradicate online child sexual abuse material.

eSafety's investigations reveal that 99% of child sexual abuse material is hosted overseas and eSafety's efforts mean that, in the vast majority of cases, content is removed in less than three days.

Image-based abuse portal and reporting tool

In October 2017, eSafety launched an image-based abuse portal. It provides reporting options, support and resources to Australians who have experienced image-based abuse, as well as their families, friends and bystanders.

Image-based abuse occurs when a person's intimate image or video is taken, shared, or threatened to be taken or shared, without consent. Often referred to as 'revenge porn', eSafety was instrumental in driving the change of lexicon to 'image-based abuse', a term that more accurately reflects the serious nature, scope and impact of this practice – and importantly, puts the emphasis on the perpetrator, not the victim.

Between 17 October 2017 and 30 June 2018, eSafety received 259 reports of image-based abuse. These reports related to 401 separate URLs and/or locations where the image-based abuse material was available across with 130 different platforms. eSafety also received 125 separate enquiries in the same period.

Despite the material often being hosted overseas, the Image-Based Abuse Team has succeeded in having material removed in 80% of cases where removal has been requested.

eSafety's research indicates that 1 in 10 Australians aged 18 years and over have had their intimates image/s or video/s shared without their consent. This increases to 1 in 4 women between the ages of 18–24 and 1 in 5 for those identifying as LGBTIQ. 1 in 4 Aboriginal and Torres Strait Islander peoples have experienced image-based abuse.[2]

As part of its comprehensive, compassionate and citizen focused approach, eSafety is working to develop specific resources that explore and address the intersectional nature of this abuse. For example, eSafety has commissioned research into the experiences of technology-facilitated abuse of women of culturally and linguistically diverse backgrounds and Aboriginal and Torres Strait Islander women.

eSafety's portal is a world first and has received both international acclaim and recognition domestically as the key point of referral for support services. Dr. Mary Anne Franks, a University of Miami School of Law Professor and Legislative & Tech Policy Director of the Cyber Civil Rights Initiative, described the portal as 'the most comprehensive resource on this issue that I have seen'[3].

Research

Through its research program, eSafety takes a leadership role in promoting, coordinating and undertaking research into digital participation and online safety issues.

eSafety's functions under the Act relating to research include efforts to:

- collect, analyse, interpret and disseminate information
- support, encourage, conduct and evaluate research, and
- publish reports and papers relating to online safety.

eSafety develops its research program through engagement with leading research agencies and other channels, including the Commissioner's Online Safety Consultative Working Group (OSCWG). This is done to ensure the program explores areas of stakeholder interest and need, and complements other research projects within the online safety space.

eSafety has released a range of research,[3] with highlights from 2017 and 2018 including:

- In October 2017, eSafety released two reports on image-based abuse – *The National Survey Summary Report*, which explored the diversity of contexts in which abuse is occurring, and *The Qualitative Summary Report*, which discusses the different views, attitudes and experience of the abuse.
- In collaboration with Netsafe (New Zealand) and UK Safer Internet Centre with the University of Plymouth, eSafety released the report, *Young People and Sexting – Attitudes and Behaviours: Research Findings from the United Kingdom, New*

[2] Office of the eSafety Commissioner, Image-based abuse national survey: summary report, October 2017 https://www.esafety.gov.au/image-based-abuse/about/research
[3] O'Brien, S.A., 'Australia takes on revenge porn', New York, *CNNMoney*, 16 October 2017, https://money.cnn.com/2017/10/16/technology/culture/australia-revenge-porn/, accessed 30 July 2018.
[3] All published research pertaining to image based abuse can be accessed via https://esafety.gov.au/image-based-abuse/about/research with other research accessible via https://www.esafety.gov.au/about-the-office/research-library

Zealand and Australia, in December 2017. The report includes eSafety's findings from the 2017 Youth Participation Survey.

- Further drawing on the findings from the 2017 Youth Participation Survey, eSafety released *State of Play – Youth and Online Gaming in Australia* in March 2018 and *State of Play – Youth, Kids and Digital Dangers* in May 2018, and
- In May 2018, eSafety released both the full and summary reports, *Understanding the Digital Behaviours of Older Australians*. The reports discuss the findings of the research that was undertaken to inform the development of the Be Connected program.

eSafety has also commissioned a range of new research to support its program delivery, educational materials and awareness activities. This research variously aims to:

- identify the type of resources and support family members, friends and peers of people aged 70 or over need to address the challenges of teaching people aged 70 or over new digital skills
- provide insight into the experiences of technology-facilitated abuse of women of culturally and linguistically diverse backgrounds and Aboriginal and Torres Strait Islander women
- understand the beliefs, attitudes and motivation of adults who exhibit image-based abusive behaviour, and
- gain insight into the attitudes and behaviours of parents and carers in relation to keeping their children safe online.

In addition to providing eSafety with an evidence base, the research team has also developed evaluation frameworks to help eSafety measure the progress and impact around our programmatic and outreach efforts.

Resources

eSafety Outreach Program

Education is an essential part of addressing complex social issues online. eSafety Outreach focuses on meeting broader community needs by providing nationally coordinated online safety education through various delivery platforms and resources.

eSafety Outreach also supports an extensive education program for school students, pre-service teachers, educators, parents, carers, community organisations, sporting groups, law enforcement, welfare agencies and mental health and youth workers.

We work directly with these stakeholders to ensure they are aware of the latest online issue trends and issues, including the threats they pose to young users and how they can be mitigated.

To ensure our program reaches a wide audience, the eSafety Outreach program uses Virtual Classrooms and webinars. These live presentations are delivered by expert trainers and include interactive elements, such as live chats and polling.

Over 2018, four main webinar events were developed for schools, including Safer Internet Day - "A better internet starts with you", the National Day of Action against Bullying and

Violence – "Imagine a future free from cyberbullying", Privacy Awareness Week – "My House My Rules" and National Child Protection Week – "Keeping Safe in the Game".

Since 1 July 2015, Virtual Classrooms have reached, and been able to positively impact, more than 240,000 Australian students and teachers.

Online materials and advice

eSafety's website, www.esafety.gov.au, is the primary destination for all Australians on a broad range of online safety matters.

As with all of eSafety's work, the available resources and services are underpinned by an evidence-based approach.

eSafety's website is divided into the following categories, which correlates with our targeted guidance according to issues and segments of the population.

- ***Young people*** – The Young and eSafe (YES) program is a youth focused web platform that is designed to engage and empower young people to take control of their online experiences. It is based on the five key themes of resilience, respect, empathy, responsibility and critical thinking and provides young people advice and support for dealing with online pressures.

  YES includes practical advice and videos, which are accompanied by lesson plans for use in the classroom. One of its short videos, "I get back up", won a Horizon Interactive Awards gold medal, recognising 'excellence in multimedia production'. Another of its materials, "Rewrite Your Story", has won awards at the World Media Festival, New York Festivals and the Australian Director's Guild. The microsite also hosts social media channels developed for young people, which includes advice on how to protect your privacy and help a friend who is being cyberbullied.

- ***Teachers*** – eSafety has developed a range of school-based educational resources and programs to assist teachers in guiding their students on how to become responsible digital citizens. This is created by eSafety's in-house team of former educators and is developed in conjunction with certification bodies and teachers.

- ***Parents*** – eSafety's online information hub, iParent, educates parents and carers on the risks their children face online. It also offers suggestions on how to initiate conversations with children on these risks and other online safety topics. The site hosts a 10 minute interactive Screen Smart Parent Tour, which is designed to help parents of 10 – 14 year olds guide their children to safe online experiences. Since launch in April 2018, over 6,500 users have downloaded 1,128 resources. The average user spends approximately 8 minutes engaging with the tour.

  iParent is updated regularly with new materials, including in relation to sexting, online gaming and gambling. In addition, there are regular blog posts, as well as updates on games, apps and social networking trends.

- ***Women*** – An online portal for women, eSafetyWomen is a 'one-stop-shop' for specialist resources for those at risk of experiencing technology-facilitated abuse, often an extension of domestic violence. The site helps women to manage the

risks of technology-facilitated abuse by providing them the knowledge and tools they need to protect themselves, whilst staying safely connected to trusted love ones and support services. This has been supplemented by the WITS online resources, which as mentioned above is our newest initiative to protect and promote women's voices online from targeted, gendered and often sexual harassment.

- ***Older Australians*** – Mature Australians are the least represented population online, but they are also the most trusting and vulnerable. The launch of a new online portal, Be Connected, helps older Australians to increase their digital knowledge, feel more confident online and protect them from attempts to scam or defraud them.

- ***Community groups*** – The eSafety Outreach Program promotes online safety and the building of digital citizenship skills across the broader Australian community. This ranges from training and resource support for the classroom to frontline services from a diverse range of community groups across Australia, including mental health and youth workers, foster carers, law enforcement and community libraries.

Be Connected

eSafety's latest research reveals Australians aged 70 years and over accounted for 74% of people—around 1.96 million people—with little or no engagement with the internet.

To help older Australians realise and maximise the benefits of being online, in November 2017, eSafety launched the 'Be Connected' website, with extensive online learning content.

Be Connected was developed in response to the Commonwealth Government's announcement in June 2016 of a $50 million financial commitment to increase opportunities for older Australians. Both eSafety and the Department of Social Services have joint stewardship of the Digital Literacy for older Australians initiative.

Be Connected is designed to specifically address the needs of those who are either digitally disengaged or have very basic skills. The learning website offers over 150 learning activities and a variety of interactive resources to help users develop basic digital skills and to interact safely online.

The next phase of Be Connected will see the portal include an additional 50 learning activities, a digital playground for seniors to practice their skills and a games area to develop mouse and keyboard skills. It will also include personalised learning plans to help older Australians safely set-up on a new device.

eSafety is expanding this initiative with a targeted outreach program to help older Australians, as well as the people and organisations who work closely with them, develop skills to stay safer online. A pilot was held in May 2018 that attracted over 200 participants, with 95% recommending the eSafety outreach program to a friend or colleague.

eSafetyWomen

eSafetyWomen empowers women to manage technology risks and abuse and take control of their online experiences through three pathways: awareness raising through targeted social media; training for frontline family and domestic violence workers; and advice and resources for women to help them stay safe online in the face of family and domestic violence.

eSafetyWomen website

The eSafetyWomen website, www.esafety.gov.au/women, features a range of 'how-to' videos giving women step by step guidance on the privacy and security features on a range of popular platforms and devices. Case studies illustrate the issues women face and how to resolve them. The website also features a personal technology check-up, as well as virtual tours of technologies commonly found in homes, cars and on mobile devices.

Training for frontline workers

eSafety delivers training to frontline workers to raise awareness of technology-facilitated abuse and provide staff with up-to-date skills and knowledge to support women and families. The face-to-face training includes a two-hour workshop that provides participants with a detailed understanding of how technology-facilitated abuse can occur, how it can be managed and how women and families experiencing or recovering from this form of abuse can be supported. Since launching in 2016, eSafety has reached more than 5,500 frontline workers across Australia.

In late June 2018, eSafety launched the *eSafetyWomen, online training for frontline workers* learning management system. This complements the existing face-to-face eSafetyWomen workshops and aims to facilitate greater access for frontline workers who may not be able to attend in-person training, particularly those in rural and remote areas. Since the release, there has been an unprecedented demand for access to the learning management system, with over 800 domestic and family violence frontline workers registering to complete the training.

The success of eSafety's women's program is reflected in the United Nations Committee on the Elimination of Discrimination against Women's ('CEDAW') eighth periodic report of Australia, which was released in July 2018.[4]

It not only welcomed the establishment of eSafety, but recommended the Australian Government 'reinforce the activities of the eSafety Commissioner to protect women human rights defenders, raise awareness of their important role in the protection and promotion of women's human rights, and protect them from rights violations by third parties'.

[4] See pages 4 and 5 of the United Nations Committee on the Elimination of Discrimination against Women's ('CEDAW') eighth periodic report of Australia, 20 July 2018, https://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CEDAW%2fC%2fAUS%2fCO%2f8&Lang=en, accessed 30 July 2018.

Women Influencing Technology Spaces

Launched as a pilot in May 2018, WITS aims to protect and promote women's voices online.

Founded on the premise that cyber abuse is not a women's issue, but rather a societal issue disproportionately affecting women, WITS draws upon the skills, strategies and stories of women for combatting cyber abuse.

eSafety developed a WITS microsite (www.esafety.gov.au/WITS), which includes:

- videos of influential women sharing stories, skills and strategies for combatting cyber abuse
- online safety tips and information for taking action, and
- a suite of newly developed resilience tips and techniques to help women build their 'psychological armour' and enhance their mental wellbeing online.

To amplify the reach of WITS, eSafety intends to host quarterly two hour-long workshops, which will give women practical guidance, including scenario based learning, on how to interact online with impact, confidence and resilience.

From the launch in May 2018 to the end June 2018, organic social media activities resulted in a potential reach of 2,000,000 with 12,400,000 potential impacts globally.

Voluntary certification scheme for online safety program providers

eSafety's Voluntary Certification Scheme for online safety program providers aims to give schools certainty that the providers they engage to deliver online safety programs are suitably qualified and experienced.

The scheme supported the Government's Project Agreement for Online Safety Programs in Australian Schools, which eSafety helped to administer.

Under this Agreement, schools in participating states and territories, which included New South Wales, Queensland, Western Australia, South Australia, Tasmania and the Northern Territory, were eligible to receive allocated funding to access online safety education from certified providers.

Thirty six online safety program providers comprising over 140 individual presenters have been accredited under the scheme.

eSafety will continue to certify providers, however a full evaluation of the program is considered timely.

Stakeholder engagement

Given the complex, dynamic and emerging field of online safety, eSafety recognises how important it is to draw upon the skills and expertise of our stakeholders.

eSafety has developed an extensive network of national and international stakeholders to support its mission of keeping Australians safer online. This is done to identify synergies and promote collaboration with key stakeholders, and ensure eSafety's projects and programs complement, rather than duplicate, existing efforts in the online space.

Key stakeholders include government agencies, industry, law enforcement, academia, not-for-profit organisations, corporations and community-based groups, with work ranging from educational materials, events, awareness raising activities and the co-development of content.

The Commissioner is also a member of the Government's National Plan Implementation Executive Group for Reducing Violence against Women and their Children and chairs the Technical Working Group of the global Child Dignity Alliance.

Further, eSafety is an active participant in the Fourth Action Plan Steering Group, which provides input, advice and support into the development of the Fourth Action Plan to Reduce Violence against Women and their Children.

eSafety's stakeholder connections are integral to our wide, proactive and whole of community preventive approach, which ultimately allows us to deliver comprehensive, compassionate and citizen focused services.

Online Safety Consultative Working Group (OSCWG)

The OSCWG provides an independent source of expert advice to eSafety. Structured into three sub-committees, its members represent industry, law enforcement, child advocacy, education, academia, not-for-profit, government and non-government organisations. OSCWG meetings are an opportunity to examine emerging policy and technological developments, as well as strategies for enhancing online safety for all Australians.

For example, in 2017, the Contact and Content Sub-committee, which among other things assists with understanding children's exposure to harmful pornography online, made recommendations in response to a request from Government for policy measures to reduce the harm being done to Australian children online from pornography.

In 2018, the Conduct and Community Sub-committee considered 'safety-by-design' principles aimed at encouraging the embedding of user safety in the design, content and functionality of digital services and products before they are deployed to market.

More broadly, OSCWG Members contribute to discussions on a variety of issues-based topics, including: shaping eSafety's approach to cyber-abuse and trolling; providing insights into issues facing LGBTQI young people; peer-based solutions for addressing negative behaviour online; and intergenerational coaching for older Australians.

eSafety and mental health steering group

In January 2018, eSafety formed the eSafety and Mental Health Steering Group (Group), to bring together representatives from Australia's key mental health and online safety organisations. The goal of the Group is to harness the collective resources of the member organisations to help combat cyberbullying and promote help-seeking strategies for individuals at risk of harm.

The Wellbeing Directory on the eSafety website is the first resource developed by eSafety, with the input of the Group, and aims to link the community to services and best practice mental health and online safety resources for Australians in-need, in an easy and efficient way.

An important goal of the Group is to shape joint research to promote positive online well-being, while influencing media messaging, including in relation to the perceived links between suicide and cyberbullying. Group members meet on an as-needed basis to rapidly respond to news stories and propose helpful media messaging that focus on help-seeking behaviours.

Prevention through Safety-by-Design

eSafety's broad remit of improving online safety for all Australians includes working with our stakeholders and industry to create safer online platforms and services.

Safety-by-Design aims to ensure that safety features are built into the design of platforms and services as they are developed, instead of being retrofitted as problems arise.

To drive this important area of work, eSafety has commenced a consultation process to establish overarching principles to form part of a Safety-by-Design framework.

This underscores eSafety's collaborative and whole of community approach to driving positive change online.

Media and communications

eSafety has developed a public profile as the source of authority, expertise and guidance on online safety issues.

As a result, eSafety is regularly asked to respond to and comment on national news stories. The Commissioner often provides comment across a range of media channels, including traditional media, social media, blogs and electronic direct mail, to amplify the message of how Australians can stay safe online.

For example, since December 2015, overall total audience growth on eSafety's social media has increased by 55%. This is a direct result of increased engagement on social platforms, including Twitter, Facebook and Instagram, which has resulted in an increase of 208% for messages sent and 145% for messages received. In the month of June 2018 alone, total number of engagements with eSafety's online activity was up 136%.

Another example is Cyberzine, eSafety's monthly electronic direct mail newsletter highlighting the latest eSafety resources and advice, which has over 10,000 subscribers, with over 320 new subscribers added each month.

This cross media approach has successfully amplified eSafety's reach and impact, especially over the last eighteen months.

For example, for Safer Internet Day 2018, eSafety engaged the Prime Minister to attend an event at Parliament House. The event was attended by over 100 guests, including

representatives from McDonalds, Optus, Telstra, the Australian Federal Police, NSW Police, Reach Out and Beyond Blue, as well as Ministers, Senators and Members of Parliament and staffers. The Prime Minister further supported the national conversation with a Facebook Live broadcast featuring the Commissioner.

Ministerial packs, including SID ribbons, were developed and sent to all Ministers, Senators and Members of Parliament to encourage support of SID in their electorates.

Social media was also used to organically reach a potential 1.18 million Facebook users and over 8.7 million potential Twitter users.

Astonishingly, an estimated 15 Million people were exposed to the important SID2018 message of improving respect, compassion and empathy online.

Conclusion

In only three years, eSafety has built a reputation, awareness and profile as the expert and authority on online safety.

Key to this is the wide, proactive and whole of community preventive approach eSafety adopts, which allows us to deliver comprehensive, compassionate and citizen focused services.

Guided by our four regulatory pillars of *Prevention*, *Protection*, *Partnerships* and *Promotion,* part two of this submission recommends changes to eSafety's regulatory framework that will enable us to more effectively and efficiently create a safe, positive and empowering online experience for all Australians.

PART 2

Question 1(a) and 1(d):

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?
and
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?

No, the Commissioner's functions and powers require expansion. Since the Enhancing Online Safety Act (Cth) ('the Act') was first implemented, and following subsequent amendments, the Office of the eSafety Commissioner ('eSafety') has paid close attention to the operability of the functions, powers, schemes and administrative structures laid down therein.

The current functions provided under s.15 have all been important to enable the Commissioner to fulfil the role's mandate. In the relatively short time since the eSafety's establishment, the Commissioner has, for example:

- supported and encouraged the implementation of measures to improve online safety for Australians (s. 15(c)), including developing a portal for reports of image-based abuse and the creation of online learning modules to increase online engagement and participation among older Australians;

- coordinated activities of Commonwealth Departments, authorities and agencies relating to online safety for children (s. 15(d)), including chairing the Online Safety for Children Working Group and hosting consultations with the mental health sector on the impact of cyberbullying on children;

- collected, analysed, interpreted and disseminated information relating to online safety for Australians (s. 15(e)), including publishing guidance material on the eSafety website, blog posts and circulating eSafety's Cyberzine;

- supported, encouraged, conducted, accredited and evaluated educational, promotional and community awareness programs relevant to online safety for Australians (s. 15(f)), including eSafetyWomen training, creation of an online training for frontline workers to assist women experiencing technology facilitated abuse, and continuing to certify providers of online safety programs;

- supported, encouraged, conducted and evaluated research about online safety for Australians (s. 15(h)), including research into youth digital participation and online safety, research into image-based abuse and research into understanding the digital behaviours of older Australians;

- published reports and papers relating to online safety for Australians (s. 15(i)), including research into parental attitudes and behaviours to keeping their children

safe online, and in collaboration with the Department of Education and Training, research to explore youth exposure to online hate; and

- monitored and promoted compliance with the Act (ss. 15(n), (o)), including promoting basic online safety requirements (s. 21) by advocating for safety-by-design and working closely with social media services.

While the Commissioner has sufficient powers to fulfil the role's mandate, eSafety has identified areas where legislative change would assist us to perform our role more effectively. These areas are largely covered in the answers to the questions in this discussion paper, and include:

- lifting constraints on the Commissioner's ability to disclose information (Q 1(b))
- expanding the Commissioner's capacity to collect, use and disclose personal and sensitive information to a level commensurate with other comparable agencies (Q 1(b))
- consolidating the Commissioner's powers by moving Schedules 5 and 7 of the Broadcasting Services Act into the Enhancing Online Safety Act. (Q 1(c))
- broadening the Commissioner's powers of delegation (Q 2(d))
- clarifying the Commissioner's responsibilities under *Public Service Act 1999*, the *Public Governance, Performance Accountability Act 2013* and other related legislation such as the *Public Interest Disclosure Act 2013* and the (Q 2(f))
- specifying that a key function of the Commissioner is to disseminate promotional and community awareness programs that are relevant to specific vulnerable groups of Australians (Q 3(b))
- specifying that a key function of the Commissioner is to advocate for and issue guidance on safety-by-design (Q 5(a))
- changing or clarifying the definitions of 'social media service' or 'relevant electronic service' under the Act to ensure that the Commissioner can facilitate the removal of cyberbullying material on a wider range of platforms and services (Q 5(e))
- expanding the cyberbullying complaints scheme to include cyberbullying targeting Australian adults (Q 5(g)).

Given the Commissioner actively uses all the functions given to her under s.15 to fulfil her mandate and that they all work cohesively to improve online safety for Australians, no function listed under s.15 of the Act should be removed.

Question 1(b):[5]

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?

Yes. eSafety believes that the current information handling and disclosure powers given to the Commissioner are not sufficiently wide, given the Commissioner's expansive remit.

The Commissioner requires broader disclosure powers to fulfil her function

The Commissioner's functions under s. 15(1)(l) of the Act include consulting and cooperating with other persons, organisations and governments about online safety for Australians. In fact, many aspects of s.15 refer to functions which rely on the Commissioner sharing information with a number of bodies, agencies and stakeholders. For example, s.15(1)(e) refers to a function where the Commissioner can 'collect, analyse, interpret and disseminate information relating to online safety for Australians' and s. 15(1)(h) gives the Commissioner the function to 'support, encourage, conduct and evaluate research about online safety for Australians'. However, current disclosure provisions do not adequately support these functions.

Disclosure of information – Part 9 of the Act

Part 9 of the Act provides that the Commissioner can disclose summaries of de-identified information and the statistics derived from de-identified information (s.85). She can also disclose in accordance with a person's consent (s.83).

Part 9 of the Act also states that the Commissioner can disclose information obtained as the result of the exercise of one of her functions or powers to:

- the Minister
- the Secretary of the Department of Communications and the Arts (DOCA) for the purpose of advising the Minister
- an APS employee of DOCA authorised in writing by the Secretary for the purpose of advising the Minister
- a Royal commission, the Director of Public Prosecutions, the ACMA and the National Children's Commissioner
- Australian Federal Police and the law enforcement authorities of states and territories
- teachers, school principals, carers, guardians, and
- overseas social media regulators.

[5] The response to question 1(c) is combined with the response to question 9(a) on page 60.

However, it is unclear whether the Act intends this list of persons and bodies to be the only persons or bodies to whom the Commissioner can disclose (that is, an exhaustive list) or merely some of them.

Part 9 was crafted for eSafety's previous remit

The permitted disclosures in Part 9 reflect the Commissioner's original remit of children, especially cyberbullying complaints targeted at Australian children. For example, permitted disclosures include the National Children's Commissioner and, if it is in respect of a complaint, teachers or school principals and parents or guardians.

The fact that Part 9 has not been expanded in line with the Commissioner's expanded remit, which now encompasses all Australians and extends beyond serious cyberbullying of children, is presenting practical difficulties, especially in respect of the Commissioner's other investigation functions. Expanding Part 9 is therefore critical to ensuring the Commissioner can exercise the full breadth of her functions and powers, including, for example, in relation to image-based abuse complaints from all Australians.

Problems with existing restrictions on disclosure

If Part 9 is interpreted narrowly, that is, that the Commissioner is only permitted to disclose information to persons and or bodies listed under Part 9, then the Commissioner's capacity to carry out her functions and activities will continue to be significantly constrained.

Difficulties experienced by eSafety include the following:

1. Inability to attain specialist ICT skillsets and harness latest technology

Contractors are not currently listed under Part 9 as parties to whom the Commissioner may disclose. This is problematic because eSafety's operations require specialist ICT skillsets which are usually only found in the contractor market and via third party resources. These specialist skill sets are vital in order to manage, maintain and support a complex PROTECTED level ICT environment, as well as to support eSafety's investigative and citizen service functions.

In addition, by not being able to utilise specialist ICT skillsets, eSafety would be constrained from harnessing new and emerging technology to effectively assist Australians. For example, eSafety is currently prevented from using cloud services to their full potential. Similarly, the capacity of eSafety to provide material to, for example, data backup services and storage facilities, remains unclear. It is arguable that because material is encrypted, its provision does not constitute disclosure, and eSafety has adopted that position in order to maintain proper operations. However, for the removal of doubt, legislative amendment is required.

2. Difficulties in workforce planning

Under s.69 of the Act, the Commissioner has the power to engage consultants. It is possible that the roles of some contractors could be structured so that they are characterised as consultants. However, the extent to the feasibility of this depends on whether the Act intends to draw a firm line between consultants and contractors. For example, it is arguable that contractors are hired to complete services and perform tasks

which are delegated to them, while consultants provide specialist advice and guidance to the Commissioner in accordance to eSafety's delivery requirements. It would be more efficient for the Act to provide abundant clarity in this matter, which would better enable eSafety to plan its workforce.

3. Inadequate defences for contractors

In addition to contractors not being referenced in Part 9 of the Act, they are also not listed as protected persons under s.91 of the Act (though consultants engaged under s.69 are). Accordingly, if a contractor comes into contact with illegal material in the process of assisting the Commissioner, this could lead to the unintended consequence of this constituting a criminal offence. eSafety therefore requests an amendment to extend the s.91 immunity to contractors.

4. Limiting eSafety's ability to collaborate on cross-government projects

eSafety's restrictive disclosure provisions have also caused difficulties in the case of cross-agency government projects. For example, eSafety collaborated with another agency as part of the Government's policy package to improve the digital confidence and skills of senior citizens. Part of eSafety's role was to collect and disclose personal information, including sensitive information, to the other agency to support their service provision of the project. While this was permissible under the more expansive information handling powers of the other agency, it was unclear whether it was permitted under the restrictive information handling framework for the Commissioner. This grey area had to be very carefully navigated to prevent eSafety breaching privacy principles or provisions in Part 9 of our Act. The Commissioner not having commensurate information handling powers with the other agencies, including those it collaborates on with government projects, is therefore presenting real and practical issues to the delivery of government priorities.

5. Limiting eSafety's ability to share information

The current disclosure framework restricts eSafety from sharing data with non-Australian entities that are not specified in s.80 of the Act such as private entities located overseas hosting cyberbullying material. This is likely to become problematic if, for example, eSafety needed to share information with such an entity in order to facilitate the takedown of image-based abuse or cyberbullying material.[6]

eSafety utilises secure data encryption methods

Relaxing the disclosure restriction in the Act would not endanger personal or sensitive information, as eSafety exercises abundant caution in handling information. For example, all guidance on secure handling of material is set out by the *Protective Security Policy Framework*. This Framework is followed by any staff handling eSafety content. eSafety also follows the provisions of the *Privacy Act* and securely encrypts sensitive data. A

[6] The Australian Medical Association, for example, in its acknowledgement of bullying being a public health issue, has stated that the effectiveness of eSafety could be improved by making it easier for the Commissioner to access relevant data from local and overseas-hosted social media services. See Australian Medical Association, 'Senate Inquiry says cyberbullying is a health issue', *Australian Medicine*, 11 April 2018, https://ama.com.au/ausmed/senate-inquiry-says-cyberbullying-health-issue, accessed 31 July 2018.

provision around disclosure in the Act is therefore is not required to ensure data sovereignty and security procedures are upheld.

Summary of suggestions for change

eSafety therefore considers that Part 9 of the Act should be amended to ensure that the Commissioner is able to collect, use and disclose the information she needs to both perform her functions and exercise her powers and assist in the achievement of broader Commonwealth objectives. The matters handled by the Commissioner are complex and sensitive and require agility, such as being able to engage contractors for all roles, to collect, use and disclose information, and to operate with other agencies at a high level. Specifically it would be desirable to:

- clarify what constitutes disclosure
- clarify and expand the arrangements under which information can be disclosed
- clarify the capacity of the Commissioner to engage contractors and the duties for which they may be engaged
- expand the Commissioner's capacity to collect, use and disclose personal and sensitive information to a level commensurate with other comparable agencies
- expand the permitted disclosures under Part 9 to accord with the Commissioner's expanded remit of all Australians, and
- extend the s.91 immunity to contractors.

Question 2(a):

Do the administrative and other provisions in the Online Safety Act provide an appropriate governance structure for the eSafety Commissioner?

No. The experience of eSafety to date suggests that the current administrative and legislative arrangements (namely Part 7 as it relates to the ACMA) are no longer appropriate as they inhibit the Commissioner's ability to perform her functions and deliver her services in the most cost effective, efficient and responsive way.

The need for eSafety to become an independent statutory Commission is preferable to support the core governance principles of clarity of purpose, transparency to the public and Parliament, and optimisation of efficiency and performance.

Currently, the Act establishes the Commissioner as an independent statutory office supported by the ACMA. In practice, this means that the ACMA provides shared services to eSafety, including payroll, insurance, human resources, facilities and IT services and support, under an agreed cost structure.

eSafety has expanded considerably in both size and remit since the Act was introduced. This is not supported or reflected in its governance structure and has created various governance and practical issues, including:

- APS compliance: there is a lack of clarity regarding whether the Commissioner is an agency for the purpose of other pieces of legislation (outlined below).

- APS framework: the eSafety Commissioner is not an Agency Head under the *Public Service Act 1999* ('the PS Act'), which limits her ability to manage her staff in respect of the APS Values and Employment Principles.

- Human resources: as all employees working for the Commissioner are employees of the ACMA, they have responsibilities under both eSafety and ACMA governance frameworks.

- Legal responsibilities: the Commissioner can delegate certain functions to ACMA staff under s.63 including entering into contracts. This is necessary for eSafety to operate efficiently in practice. However, arguably this can cause confusion, with parties unsure whether they are contracting with eSafety or the ACMA, due to the absence of an eSafety Commission.

- People management: as all employees working for the Commissioner are subject to the terms of the ACMA Enterprise Agreement, people management decisions are not able to be made within eSafety, thus impeding the capacity of eSafety staff to be employed under arrangements fit for eSafety's functions, including the need to be responsive to citizens after hours.

- Finance issues: the Commissioner is not an accountable authority under the *Public Governance, Performance and Accountability Act 2013* ('the PGPA Act'), which limits her ability to manage her resources in the most fiscally prudent and responsible way.

- Budget: eSafety's budget is provided to the ACMA rather than eSafety, giving the ACMA the responsibility for reporting on eSafety's expenditure, which reduces the Commissioner's transparency and accountability to the public and Parliament.

- Information Technology: as the ACMA and eSafety have a shared services arrangement, Safety is reliant on the ACMA in the information technology space. However, the ACMA has faced difficulties in providing the specialised security and faster response times which are essential due to the sensitive matters eSafety handles and its citizen-facing services.

As outlined above, there is considerable ambiguity and inconsistency regarding the Commissioner's obligations, and those of ACMA staff assisting her, under the key legislative schemes regulating the operations of the public service.

For example, the explanatory memorandum to the Act states that the eSafety Commissioner is an agency for the purposes of the *Privacy Act 1988*. The explanatory memorandum also states that the Commissioner has certain exemptions under the *Freedom of Information 1982* ('the FOI Act'). However, it does not specify whether the Commissioner is an agency for the purposes of the FOI Act. Similarly, the explanatory memorandum does not outline the Commissioner's obligations under the *Public Interest Disclosure Act 2013* ('the PID Act'), including whether the Commissioner is considered an agency for the purposes of the PID Act. It therefore remains unclear how someone seeking to make a disclosure regarding the Commissioner would proceed.

Common to the issues outlined above is the lack of clarity and connection between the Commissioner and the staff and functions she manages. As outlined further in 2(f), making the Commissioner an accountable authority under the PGPA Act and an agency head under the PS Act would be the basis of a more efficient and fit for purpose governance structure for eSafety. This will ensure that the Commissioner is solely responsible and has direct authority over all her operations and expenditure. This would remove the risk of another agency (in this instance the ACMA) from holding responsibility against the Commissioner on matters over which the ACMA Chair in practice has no visibility or oversight.

Further, given eSafety's expanding remit, the unique leadership and coordination role it plays in the online safety space, and its existing and growing public profile as the entity with authority on cyber safety, the eSafety Commission should be established as an independent agency. As part of this arrangement, staff assisting the Commissioner would become eSafety staff forming an agency with the eSafety Commissioner, rather than being ACMA staff assisting the Commissioner. This would ensure eSafety can continue to evolve in a nimble and agile way. This is fundamental if eSafety is to keep up with the dynamic, complex and fast paced nature of the technology industry.

Establishing the eSafety Commission, combined with giving the Commissioner greater autonomy and accountability, would place eSafety in a position of strength to proactively and efficiently address online safety issues for the benefit of all Australians.

Question 2(b):

Is the ACMA still best placed to provide administrative support to the eSafety Commissioner?

No. In addition to the above response, eSafety and the ACMA's roles have changed considerably since the inception of the eSafety Commissioner. The organisations have different stakeholders, risk profiles, ICT security needs and infrastructure requirements, different human resources arrangements and work patterns, and require different skill matrices from their respective staff. Further, the highly sensitive and complex nature of the material and matters within the eSafety remit requires unique strategic approaches and highly specialised staff.

Since inception, the role, functions, and subsequently the size of eSafety have been significantly extended so that there are now strong arguments for the Commissioner to operate as a separate and independent entity. The field of online safety has a landscape unparalleled in its volatility: players, offences, solutions and technologies all change swiftly.

The compatibility of regulatory function and policy endeavour which saw the creation of eSafety from ACMA has been superseded by technological change and eSafety's expanded remit, including the addition of increased citizen facing services. The synchronicities which previously made the arrangement cost effective have been superseded. A more suitable model necessitates administrative independence.

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?

Yes. Establishing governance arrangements that give the Commissioner greater autonomy and accountability will assist in addressing and remediating the issues outlined above.

eSafety staff are employed under the ACMA enterprise agreement. The enabling legislation, when combined with the existence of this agreement, generates an administrative framework which has the effect of preventing the Commissioner from efficiently managing her own staff in order to most effectively perform the functions assigned to her in the Act.

Section 63 permits delegation by the Commissioner to a member of ACMA staff, while s.68 states that the Commissioner is not subject to direction by the ACMA in relation to the performance of a function or the exercise of a power. This precludes the Commissioner receiving delegation of functions from the ACMA Chair. While the Commissioner's staff could technically receive some delegations from the ACMA Chair, it is unclear how this would work in practice, and of course this approach does not reflect the practical reality that ACMA employees allocated to the eSafety take direction from the Commissioner.

The ACMA enterprise agreement requires the Chair or her delegate to deal with matters as varied as extended medical leave, Individual Flexibility Agreements ('IFAs'), approval of home based work, part time or overtime. It is arguable that this creates unnecessary duplication, negotiation and discussion when ultimately it is logical that this decision making should solely rest with the Commissioner. Further this would enhance operational efficiency and clarity. Under the current administrative arrangements the ACMA Chair or her delegate in practice is required to make such decisions with little visibility or supervision over the operational requirements of eSafety.

The Commissioner is best placed to formally decide on the necessity and suitability of such matters. It is also reasonable for the Commissioner to manage any requests or issues associated with the staff that she leads.

While the ACMA Chair is legally responsible for the regulation of these staff-related matters for ACMA employees, including, therefore, those in relation to staff assisting the Commissioner, in practice, the Commissioner is responsible for the day to day management and administration of these matters. This therefore makes the current arrangements difficult and undesirable for both the Commissioner and ACMA Chair.

It is also important for the Commissioner to have more certainty and permanence associated with the long-term management, training and investment in her staff. The current situation means that staff who work for the eSafety Commissioner pursuant to s.67 might be considered similar to APS staff seconded to a different agency, and the arrangements surrounding their management are insecure and subject to external factors.

The ACMA has complete oversight and decision making authority over all human resource and operational policies and procedures. eSafety staff as ACMA employees must adhere to these policies. This is not ideal or practical given they do not always adequately account for the unique operational requirements of eSafety.

The ACMA Enterprise Agreement as it currently stands does not accommodate the specialist skills and different working arrangements required to carry out some of the eSafety functions. For example, eSafety staff will often need to assess and respond to complex and sensitive cases outside of core business hours. During October 2017 to 30 June 2018 over 60% of Image Based Abuse reports were received outside of business hours.

eSafety is also tied to decisions made by ACMA with respect to funding, office location, rent, and security arrangements. This can cause practical difficulties: for example, the growth associated with eSafety's expanded remit means that new space is urgently required. However, eSafety does not have any control over its use of space; it does not have the ability to forecast or plan ahead as its allocation is contingent on the needs of the ACMA.

These factors substantially impede eSafety's capacity to shape its own strategic direction or to operate in an agile manner to provide the highest quality and greatest number of citizen services. Further, it is out of step with the fact that the ACMA and eSafety no longer have the functional and policy synergies that once existed.

For these reasons it is timely for the Act to be amended to create an independent statutory agency for the office of the eSafety Commissioner.

An instructive model may be found in the *Ombudsman Act 1976*. The Office of the Commonwealth Ombudsman is classified as a 'small agency'. Under s.31, the staff of the Ombudsman are engaged under the PS Act rather than under the enabling legislation of a particular agency. This promotes clarity, and consistency across the public service with associated efficiencies. The Ombudsman and the APS employees assisting the Ombudsman together constitute a statutory agency; and the Ombudsman is the head of that statutory agency. Under s.4A, for the purposes of the finance law (within the meaning of the PGPA Act), the Commonwealth Ombudsman is the accountable authority of the Office of the Commonwealth Ombudsman and the Ombudsman's staff are officials of the Office of the Commonwealth Ombudsman.

Similarly, the Australian Organ and Tissue Donation and Transplantation Authority is an 'extra small agency' with fewer than 30 employees. It has a Board as accountable authority (see s.8 *Australian Organ and Tissue Donation and Transplantation Authority Act 2008*), its own enterprise agreement, and a service level agreement with the Department of Health.

The provision of budget directly to eSafety, and not through the ACMA as per the current process, would reduce reporting issues where eSafety is required to spend considerable time and effort providing representations to the ACMA about the appropriate use of funds. The ACMA must report on eSafety's financial position yet has limited control over this. Additionally, the separate provision of funds directly to eSafety would ensure clarity regarding apportionment of savings measures that are assigned at agency level.

Question 2(d):

Does the eSafety Commissioner require a broader delegation power? If so, how would it be limited?

Yes. Section 63 of the Act provides the Commissioner with only limited powers to delegate to ACMA staff, and does not allow the Commissioner to delegate to contractors.

Delegations that would permit eSafety to employ contractors to take on after hours/weekend work, for example, in relation to cyberbullying or image-based abuse, would enhance the capacity of eSafety to provide compassionate citizen services and more comprehensive online safety support for Australians.

Victims of cyberbullying and image-based abuse would especially benefit from the Commissioner having a specific power to delegate to contractors. As it stands, the existing powers of delegation do not allow eSafety to respond to victims outside of business working hours – times we know that victims are very much in need.

Between mid-October 2017 and 30 June 2018, approximately 60% of image-based abuse complaints eSafety received occurred outside business hours. In the last two months, eSafety has found that approximately 50% of cyberbullying complaints are reported outside business hours.

Further, eSafety would be more readily able to achieve its statutory objective of promoting online safety for all Australians if the Commissioner was given powers commensurate to those of other agencies in relation to delegating power as is necessary to fulfil a function or activity. This would support with s.16 of the Act, which states that 'the Commissioner has power to do all things necessary or convenient to be done for or in connection with the performance of his or her functions'.

Question 2(e):

Should the eSafety Commissioner consider delegating some or all functions to a body corporate?

No. Some of the Commissioner's functions are unsuitable for delegation to a body corporate, and her functions are also most appropriately held by government.

Section 64 of the Act enables the Commissioner to delegate to a body corporate any or all of her functions or powers relating to Part 3 ('Complaints about cyberbullying material') or Part 4 ('Social media services'), with the exception of s.35 ('social media service notice') or s.37 ('formal warning').

This means that it would be possible under the Act for eSafety to delegate to a body corporate the handling and investigation of cyberbullying complaints of children, administration of the Tier Scheme and communicating and promoting compliance with basic online safety requirements. However, such a delegation would not be appropriate and as such s.64 does not require expansion to facilitate delegation of any other powers to a body corporate.

A key reason for this is that an important role of government is to protect and promote the wellbeing of its citizens. One method of doing so is by creating and distributing free resources to a diverse community with differing and at times, complex needs. Government is arguably best placed to alleviate the circumstances of vulnerable citizens, including for example persons experiencing domestic violence, people from culturally and linguistically diverse backgrounds, children and young people, and people with disabilities.

Certainly, non-government entities can play a valuable role in assisting citizens to stay safe online. However, often the services provided by such entities do not involve enforcement and/or regulation, which are integral to the work of eSafety and support its success in delivery for Australian citizens. For example, New Zealand's Netsafe does not have the capacity to exercise regulatory functions. This is the role, and responsibility, of government. eSafety has the ability to exercise regulatory, and if necessary, enforcement functions to combat image-based abuse, cyberbullying, and removal of illegal content. eSafety as a governmental regulatory body is therefore uniquely placed to regulate and influence an ever-evolving industry.

This is not to say that eSafety operates in isolation. We strongly believe that dealing with online safety issues requires a whole-of-community approach. This is best facilitated and led by a federal government body but involves working in close collaboration with communities, the not-for-profit and community sectors as well as with other key stakeholders. Such joint efforts enable communities to effectively combat the multiple and complex concerns faced by Australians online, ensuring:

- a cohesive nationally led approach to the delivery of services and programs
- mitigation of resource duplication
- the capacity building in relevant sectors to strengthen prevention programs and responses to online safety
- that online safety issues are addressed using multiple strategies, including primary prevention through education, secondary prevention by creating resources and programs to assist in the early detection of risk, and tertiary prevention by equipping professionals and victims with immediate solutions, and
- the provision of free, high quality materials made accessible to broad audiences, particularly vulnerable Australians.

eSafety's *Be Connected* joint initiative with DSS, a learning management portal to increase digital engagement and participation among older Australians, was developed in close consultation with a range of specialist community sector organisations to address the fact that that many existing resources targeting older Australians were of varying quality and limited in reach. By adopting a collaborative approach, eSafety has ensured that there is no duplication of tools and that the portal makes available a complementary suite of learning resources. Since its launch nine months ago, almost 45,000 users have undertaken learning opportunities and importantly, over 90% of users of Be Connected have reported (since completing the program activities) feeling confident to apply the skills they have learnt and are inspired to learn more.

The success of our eSafetyWomen training for frontline workers is another example of the benefits that a government-led program with a national focus can have. eSafety consulted extensively with key stakeholders to supplement our own research and subject matter expertise to produce a resource that not only addresses the requirements of those in need but is also recognised as a valuable capacity building tool for the sector. Similarly, eSafety has recognised the positive contribution of the eSmart initiative of the Alannah and Madeline Foundation and has kept its own focus on virtual classrooms as part of its outreach program. eSafety has also benefited from collaboration with the Children's Commission, and rather than creating its own Youth Advisory Council has welcomed the opportunity to seek advice from the Children's Commissioner through the Online Safety Consultative Working Group.

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?

No. As discussed in 2(a), eSafety's governance structure is not fit for purpose for eSafety's functions and one of the key issues is that the Commissioner is not an accountable authority under the PGPA Act or an agency head under the PS Act.

Currently, all staff reporting to the eSafety Commissioner are employees of the ACMA. The ACMA Chair is an accountable authority under the PGPA Act. Her duties include ensuring sustainable and proper management of public resources and establishing and maintaining systems relating to risk management and control, including a risk management policy and framework. Similarly, an agency head under the PS Act is responsible for the general management and leadership of APS employees within their entity.

However, the present legislative arrangements do not reflect practical operations. As discussed above, while the ACMA Chair is legally responsible for the regulation of these matters in relation to ACMA employees assisting the Commissioner, in practice, the Commissioner is responsible for the day to day management and administration of these matters. This means ACMA employees assisting the Commissioner operate within the obligations of, and have responsibilities under, the legislative structures of two agencies at various times, on various matters. This duplication and inconsistency undermines the efficiency of eSafety's operations and performance.

The Commissioner is better placed to manage her staff and have comprehensive and robust oversight of eSafety arrangements. Making the Commissioner an accountable authority under the PGPA Act and an agency head under the PS Act would therefore provide a number of benefits.

First, it would provide clarity and consistency to the Commissioner's governance arrangements. Second, it would drive efficiencies in operations and performance. Third, it would make the Commissioner more accountable and transparent to the Parliament and public. Fourth, as the Commissioner already in practice manages and acquits many PGPA Act and PS Act responsibilities, it would ensure practical arrangements reflect legislative obligations.

Further, as two of the cornerstone legislative schemes regulating the management of the public service, establishing the Commissioner's obligations under the PGPA Act and PS Act should assist in clarifying her obligations under the other legislative schemes. This is especially the case if the eSafety Commission is established as an independent agency with eSafety staff.

Question 3(a):

Has the eSafety Commissioner been effective in enhancing online safety for children since its establishment in 2015?

Yes. Since its establishment, eSafety has effectively worked to enhance young people's online safety through a multi-faceted approach, combining preventative education with early intervention and harm minimisation.

The wide, proactive and whole of community preventive approach eSafety adopts, which allows us to deliver comprehensive, compassionate and citizen focused services to children, includes:

- conducting evidence-based research into online safety trends and the information needs of young Australians
- providing solutions-focused online safety guidance and developed tailored, age specific programs to reach hundreds of thousands of Australian children and their families
- providing direct support and relief to Australian children by resolving over 900 complaints of serious cyberbullying, and referring thousands of others to help services, and
- working with our international partners to facilitate the removal of over 20,600 URLs providing access to child sexual abuse material.

eSafety provides a one-stop shop for online safety, with a range of functions that inform and support each other to drive tangible and positive change for children. For example, our 2016 'Social Cohesion' research indicated that participation in an online safety education session increased students' capacity to report cyberbullying and other concerns.

As a national agency, we effectively coordinate and lead the online safety community and provide authoritative messaging on complex and emerging cyber issues relating to children. For example, eSafety's understanding of the complexities of both protecting and empowering children online is an area of expertise that is particularly sought after and trusted by our key audiences and stakeholders.

Education and awareness

Education and awareness is the cornerstone of eSafety's preventative approach. While the primary audience for education programs is young people, in recognition that a whole-of-community approach is needed, programs also target parents, carers, educators and others who have a key role in supporting children, as critical secondary audiences.

User uptake indicates the extent of our reach and the value educators find in our curricular resources. Our education and online safety information resources are our most accessed pages on our website, with over 2,990,000 page views and approximately 1,800,000 users. Our dedicated iParent website has attracted 531,000 page views and 387,000 users. Our new Screen Smart Parent Tour, launched in April 2018, has user interaction at an average of 8 minutes per visit. Our Screen Smart Parent Tour in particular received positive feedback from teachers and the support sector, with participants saying that the Tour is easy to use, engaging and practical for time poor parents and carers and is rich with ideas on how to keep children safe online.

Over 350,000 Australian children, teachers, parents, carers and community members have participated in online or face-to-face training sessions. Our Virtual Classrooms ensure primary school students can access at least four different sessions per year without leaving their classroom. The popularity of this program is increasing each year. In 2017, 61,000 students participated and in the first half of 2018, this increased to 111,000.

eSafety's own research and external findings indicate teacher support and professional development is a protective anti-bullying intervention. 9,059 attendees have participated in our Pre-service Teacher Training, (for those in their last year of teacher training), while our Teacher Professional Learning in 2017 reached 1,331 teachers. In 2018, we will double those numbers, with 1,052 teachers already participating and a further 1,259 booked in for Term 3 webinars. NSW Department of Education has requested that all its teachers have access to this free, high quality online safety education and are rolling out a pilot, offering the program to all NSW Department schools as part of December 2018 staff development day. The Teacher Professional Learning program has provided accessible high quality online safety education to communities difficult to reach and other stakeholders, including casual relief teachers. 96% of participants in this program have rated it as 'excellent' or 'good'. eSafety has also received positive qualitative feedback, informing us that our training easily translates into practical know-how for participants.

'The program raised my awareness of the often 'hidden' nature of cyber bullying and of the need to monitor my classes and students a little more closely. The take away for me was the importance of reporting and of the need to be familiar with the reporting process to be best able to assist the children I teach. I will also be promoting this knowledge among fellow staff.'

'Clearly up to date with the latest issues students and staff are facing. Friendly way of communicating the issues making me feel competent and enabling me to be more aware with what's going on online.'

'I am very impressed with the support material that is available and I will use this to integrate rich and real learning experiences to support the children in preventing and managing cyberbullying.'

Online delivery enables scalability, interactivity and engagement coupled with obvious time and cost benefits. It allows for the tracking of attendance, real time polling and provides an instantaneous feedback loop to eSafety. The value of government in creating and delivering content is particularly necessary in rural and remote areas, where the number of children, parents, carers and teachers are often too small to justify the efforts of not-for-profits and others to travel and deliver eSafety content. To accommodate this, eSafety has looked for opportunities to fill this gap and scale the delivery of content.

Program development and roll out

In addition to our direct engagement with schools and young people, eSafety is informed by a number of internal and external intelligence sources in determining how it can be most effective in enhancing children's online safety.

eSafety's extensive research program provides current, nationally representative data on the nature and prevalence of online safety issues experienced by young people, along with the strategies they are currently using to stay safe and where they need additional support to thrive in the online environment. In 2018, eSafety's most recent report, *'State of Play – Youth, Kids and Digital Dangers'*, identified the top negative experiences and the ongoing impact – positive and negative - that these experiences have had on young people.

eSafety has an intimate knowledge of the online safety landscape including a deep understanding of the specialties offered by others. We work through stakeholder mechanisms and formal and informal working groups such as the Online Safety Consultative Working Group, the eSafety and Mental Health Steering Group, and regular liaison with State and Federal education agencies. Through these mechanisms we are made aware of existing specialties and best-practice programs. For example, in the non-government sector, Project Rockit focuses on direct youth engagement, the Alannah and Madeline Foundation develop and deliver a preventative framework to schools and libraries through the eSmart program, and Beyond Blue and Headspace are rolling out the National Education Initiative focusing on broader issues of mental health for young people. We do not seek to duplicate these existing efforts.

We seek to fill gaps where there is a demonstrated need and we have the competencies to ensure effective delivery and take-up of our programs. For example, the online delivery of our Virtual Classrooms and Teacher Professional Development ensures children and teachers regardless of location (including in remote and regional Australia) can access high quality online safety training. Our Pre-Service Teacher Training is not offered by other providers. Our education resources fill gaps in existing curriculum materials, and we consult with the Australian Curriculum, Assessment and Reporting Authority ('ACARA') and teacher standards bodies to ensure resources meet the needs of students and teachers. Our forthcoming YeS Project, a peer support and mentoring project intended to upskill young people to be a force for positive change in the online space, will fill one of those program gaps.

At the Federal level, eSafety works with Education Services Australia to feature its programs on the Student Wellbeing Hub and the Bullying No Way! website. This ensures national reach and visibility of programming. At the State level, eSafety is in regular contact with State Education Departments and Catholic and Independent agencies to ensure awareness of and active promotion of our programs.

Program effectiveness

eSafety draws upon its own research and experience, along with available national and international evidence into what constitutes best practice, so that its online safety education program stays relevant and effective.

The body of evidence into what types of interventions are most likely to drive and effectively measure behavioural change in the online environment indicates that the type of interventions that work best[7] include those that:

- allow multiple exposures to online safety messages, using varied educational platforms
- provide for a focus on specific skills, including social and emotional skills, along with opportunities to practice these skills
- target early education, prior to the onset of the intended behaviour
- are led by well-trained educators
- employ a holistic, whole of community approach, and
- employ monitored implementation and improvement of programs through evaluation.

In designing and delivering education programs, eSafety seeks to deliver against the above criteria. For example:

- educational content is made available through multiple channels including videos, games, discussion posters, and online presentation-style formats
- classroom resources, including the award winning Rewrite Your Story (World Media Festival, New York Festivals and the Australian Director's Guild) and the Young & eSafe site, provide opportunities for young people to practice social and emotional skills of responsibility, resilience, reasoning, empathy and respect online
- upskilling of educators occurs through the Teacher Professional Learning and Pre-Service teacher programs
- programs are tested extensively with target audiences prior to implementation, and monitored and evaluated through feedback loops and pre-and post-implementation surveys, and other evaluative tools, and
- a broad community focus is promoted through resources such as the iParent portal, helping parents and carers understand online risks and how to manage these risks.

Cyberbullying complaints scheme

In addition to its preventative education program, eSafety's cyberbullying investigation function provides a mechanism for early intervention in situations where young people have experienced a harmful cyberbullying incident.

Since July 2015, eSafety has managed a complaints scheme for serious cyberbullying of Australian children. This scheme provides invaluable support and technical assistance to

[7] https://www.cese.nsw.gov.au/publications-filter/anti-bullying-interventions-in-schools-what-works https://www.fosi.org/policy-research/increasing-youth-safety-responsible-behavior/

complaints, including to Australian children and young people, their parents, carers and other adults who make complaints on their behalf. eSafety received and assessed a total of 900 cyberbullying complaints between July 2015 and 30 June 2018.

There has been a significant year-on-year growth in the number of complaints we receive as awareness of eSafety's cyberbullying role has increased, from 186 complaints received in 2015-6 to 305 in 2016-7 and 409 in 2017-8. Through our relationships, escalation pathways and formal powers, eSafety has been able to effect the rapid removal of serious cyberbullying material on social media services impacting on the mental health of young Australians (such as harmful comments, incitements to suicide and threats of violence) often within hours or a day.

Besides the practical assistance we provide, we know that just being able to speak to someone from eSafety can provide significant comfort for cyberbullying victims. We also work with schools where appropriate to address the inter-personal behaviours that often underpin cyberbullying, and with law enforcement in the most serious cases. Our website has also provided a valuable resource to Australians seeking help and support and Kids Helpline has received over 7,000 website visits from people through the eSafety website.

The opportunity to interact directly with young people impacted by cyberbullying enhances our understanding of what works best in alleviating harms and improving young people's online experiences. Such interactions have also allowed eSafety to receive positive feedback regarding the work of our cyberbullying team. Children, young people and their parents and carers have expressed their appreciation at the speed and skill with which their complaint was handled.

"A very big thanks for your call yesterday and the assurance and comfort you provided."

"I would like to sincerely thank you again for all of the assistance you have provided us with. Your follow up has been incredibly responsive and I have appreciated your calm manner and considered advice."

"Thank you for your support, I am very thankful that a service like this exists especially when this is my first experience with an incident of this nature".

"Thank for your amazingly quick response. My child is secure, happy and safe and I appreciate your response."

Such feedback highlights the continued importance of providing empathetic, timely and practical responses to children and young people hurt online, and the differences such responses can make to children and their families.

Online Content Scheme

Through its CyberReport team eSafety also operates the Online Content Scheme, which works to keep children safe through mechanisms that restrict access to content that is inappropriate for children. These mechanisms are attached to the FFFS, which promotes end-user device-level filters that operate in part, based on the set of prohibited URLs generated by the eSafety Commissioner through its complaints scheme.

In addition, eSafety works with the INHOPE network to rapidly remove large volumes of child sexual abuse material from networks around the globe. Child sexual abuse victims are re-

traumatised through the knowledge that content memorialising their abuse remains in circulation on the Internet. We, and our INHOPE partners, prioritise CSAM in the knowledge that its removal can significantly assist victims to move onto the road to healing and moving forward with their lives.

In 2017-18, the CyberReport team concluded 8,040 reports into online CSAM, 7,736 of which were referred to INHOPE for takedown. This was a 57% increase on the year before. In total, INHOPE members exchanged 87,930 reports, with the vast majority of material removed in its host jurisdiction within three days.

Finally, the CyberReport team manages effective relationships with a range of Australian law enforcement agencies. These relationships are formally expressed in memoranda of understanding (MOUs) concluded with every state and territory police force, and the Australian Federal Police. The MOUs set out when the eSafety Commissioner will refer content that is sufficiently serious to warrant attention by law enforcement to Australian police. The agreements also specify that the eSafety Commissioner will defer regulatory action in appropriate circumstances to ensure that a police investigation is not prejudiced. For example, if the eSafety Commissioner concludes that CSAM is hosted in a particular Australian state, that jurisdiction's relevant specialist command will be notified. Action will not be taken to initiate takedown of the content until the specialist command has confirmed that on-foot investigations will not be compromised by its removal. In addition, where it appears that CSAM shows that a person (for example, an offender or victim) is located in a particular state, then the eSafety Commissioner will also notify that content to the relevant specialist command.

Case Study

In 2017, a CyberReport investigator reviewed a video file showing a male adult sexually abusing a child of around three years of age. Based on his accent and vernacular, the male appeared to be Australian. The male sported a number of distinctive tattoos, and the high-resolution video file allowed the CyberReport investigator to capture clear screenshots of the designs. Video background detail indicated that the male was likely in a specific state, and the screenshots were shared with police detectives in that state. Using the screenshots and the male's physical description, police identified the male, who was serving a prison sentence for child sexual assault. At the time of referring the matter to police for further investigation, detectives were considering laying further charges against the male.

Under an agreement with the AFP Commissioner, the eSafety Commissioner notifies all CSAM URLs provided from an INHOPE-member country to the relevant INHOPE hotline for takedown. Non-INHOPE CSAM URLs and all pro-terror content is notified by the eSafety Commissioner to the AFP. In addition, the eSafety Commissioner will also immediately notify the AFP in cases where information is encountered that may lead to the identification of a person (e.g. an offender or victim) who appears to be based overseas.

Feedback and remit expansion

More broadly, the effectiveness of eSafety's approach is evidenced by the reputation, awareness and profile it has built with its stakeholders and the Australian community. For example, the Legal and Constitutional Affairs References Committee took extensive testimony and feedback from the Australian community for its inquiry into the adequacy of existing offences in the Commonwealth Criminal Code and of state and territory criminal

laws to capture cyberbullying (Senate Cyberbullying Inquiry).[8] Overwhelmingly, feedback both supported and valued the work of eSafety. The Committee ultimately recommended that eSafety be adequately resourced, actively promoted to the public and provided with additional legislative amendments to bolster its effectiveness.
The increasing demand for our resources and services, as well as our growing external profile, further supports that eSafety has been successful in raising awareness of online safety issues for children and acting as a safety net for Australian families.

Lastly, and ultimately, the fact that eSafety's remit was expanded in July 2017 was a recognition of how effectively it had fulfilled its original remit and an acknowledgment that its support, guidance and expertise should be provided to all Australians.

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?

Yes. eSafety considers the expanded scope of the Online Safety Act has been helpful in relation to groups other than children, and has enabled eSafety to also provide for the online safety needs of all Australians, particularly more vulnerable groups of our community. These groups include women at risk of experiencing technology-facilitated abuse or serious online abuse, Australians impacted by image-based abuse, and older Australians. But that said, since the expanded remit did not come with enhanced resources or extension of the legislative schemes to compel take down, the services we have provided to assist other groups has been done where and when we have capacity and, in some cases, through unfunded programs and initiatives.

Below, we outline some of the programs and initiatives we have developed and rolled out to help vulnerable Australians, beyond children.

eSafetyWomen

The eSafetyWomen program was made possible by funding from the Women's Safety Package to Stop the Violence. This funding ceased at 30 June 2018 however an additional $1.2 million over four years has been received to maintain the program. Our eSafetyWomen program aims to empower Australian women to manage technology risks and abuse and take control of their online experiences through two major initiatives – the eSafetyWomen website and training for frontline workers. The *ReCharge: Women's Technology Safety - National Study* findings state that 98% of clients had experienced technology facilitated-stalking and abuse as part of their domestic violence experience. The eSafetyWomen website—www.esafety.gov.au/women—features helpful 'how-to' and case study videos, a personal technology check-up and virtual tours of technologies commonly found in homes, cars and mobile devices. Almost 84,000 people have visited the website and viewed more than 193,000 pages of content.

eSafety delivers workshops to frontline workers to raise awareness of technology-facilitated abuse and what can be done in response. eSafety also offers online training for frontline workers to facilitate greater access for frontline workers who may not be able to

[8] Senate Legal and Constitutional Affairs References Committee, Report, Adequacy of existing offences in the Commonwealth Criminal Code and of state and territory criminal laws to capture cyberbullying, March 2018

attend workshops (particularly those based in rural and remote areas) and as a valuable additional resource for those workers who participate in the workshops.

eSafety has seen strong demand for the workshops, having so far run over 300 workshops reaching more than 5,500 frontline workers. The workshops are well-received by frontline workers with 82% of respondents to the post-workshop survey rating it as 'excellent'. Although the online training was only launched at the end of June 2018, over 800 domestic and family violence frontline workers have registered to complete the training.

eSafety is currently exploring how best to cater for the needs of Aboriginal women, particularly those living in urban areas, women from Culturally and Linguistically Diverse Backgrounds, and women with disabilities. All of this future work will be underpinned by research and executed through partnerships with organisations working in these communities.

Women Influencing Tech Spaces

Launched as an unfunded pilot program in May 2018, Women Influencing Tech Space ('WITS') aims to protect and promote women's voices online. It draws upon the stories, skills and strategies of women to combat cyber abuse, a societal issue that disproportionately affects women, and empower women to interact online with impact, confidence and resilience.

The WITS website (www.esafety.gov.au/WITS) has a range of unique resources, including videos of women sharing their stories of combatting cyber abuse, information for taking action and resilience tips to help women build their psychological armour.

From the launch in May to the end June 2018, organic social media activities resulted in a reach of 2,000,000 individuals with 12,400,000 potential impacts globally.

To amplify the direct reach and impact of WITS, eSafety intends to host quarterly workshops with partners in the corporate and NGO community, to give women practical guidance and support on how to interact online confidently and safely.

Image-based abuse portal

In mid-October 2017 eSafety introduced its image-based abuse portal to give tangible support to Australians who have had their intimate images or video shared without their consent.

The portal is a place where Australians can report image-based abuse to seek its removal, and access practical advice and resources to help them manage the impacts of image-based abuse.

Between 17 October 2017 and 30 June 2018, eSafety received 259 reports of image-based abuse. These reports related to 401 separate URLs and/or locations where the image-based abuse material was available across 130 different platforms. eSafety also received an additional 125 enquiries about image-based abuse. The portal was visited over 91,700 times in this period.

eSafety has been successful in having image-based abuse material removed in 80% of those cases where removal has been requested, despite the material being hosted overseas and in the absence of formal powers.

A bill before Federal parliament seeks to introduce a prohibition on the posting or threatened posting of intimate images and to establish a complaints and objections system that eSafety will administer, which should further increase eSafety's effectiveness in tackling image-based abuse. [9]

Be Connected – Digital Literacy for Older Australians

In November 2017, eSafety launched the Be Connected learning management portal (website) to increase digital engagement and participation among older Australians, a group that faces barriers to accessing important services and enjoying social interaction online, and is at risk from isolation and fraud.

The Be Connected website has information and interactive training tools and resources for older Australians, their families and peers, and local community organisations. The website is complemented by a network of trainers providing face-to-face assistance. Since launching in November 2017, 43,486 people have used the website taking part in has more than 90,000 training sessions. Over 90% of users report finding the material engaging and interesting and feel confident to apply the skills they have learnt through the portal.

Be Connected is a joint initiative of eSafety and the Department of Social Services to improve digital literacy for older Australians.

Outreach to all Australians

In addition to the Outreach noted in Question 3(a), eSafety also provides online and face-to-face training and preventative education to a variety of adult audiences. The aim of the training is to raise awareness of the role and functions of eSafety, to share current technology trends and provide targeted online safety advice. Over 15,600 people including mental health and social workers, library workers, law enforcement, corporates, not-for-profits and sporting organisations have been upskilled through this direct outreach. eSafety sees preventative education as the key to changing online behaviour both for young people and adults.

eSafety also continues to identify groups in the community that have particular online safety needs and to work to address those needs. For example, in partnership with the Department of Prime Minister and Cabinet, eSafety is creating a digital literacy and online safety app for Aboriginal and Torres Strait Islander peoples in remote communities. The app will provide tailored advice on digital skills most relevant to people in Aboriginal and Torres Strait Islander communities, including device and digital literacy and safety. This complements our popular animation and poster resource, Be Deadly Online, which was developed with Aboriginal and Torres Strait Islander writers and voice actors, and which we hope to refresh shortly. Other groups earmarked for future program development include women from CALD communities as well as individuals with disabilities.

[9] Enhancing Online Safety (Non-consensual Sharing of Intimate Images) Bill 2018.

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?

Yes. eSafety considers that online safety in Australia is addressed in a way which strikes a balance between equipping Australians to identify, assess and self-manage online risks and targeted government intervention.

In our view, the most effective measure to address online risks is prevention by equipping Australians to manage their online experiences. However, there is always a role for government intervention to minimise harm when concerning content or troubling behaviour is found online, or when an inherent power imbalance may exist between online service provider and user.

The Act recognises that prevention can take a number of forms by conferring a range of relevant functions on the Commissioner such as promoting online safety, coordination of activities, and research.[10] Under these functions, eSafety has been able to provide a wide range of resources to empower all Australians with the knowledge and skills they need for better online interactions and to encourage industry to do likewise.

For example, eSafety provides:

- Evidence-based education programs and resources for educators, parents, carers and young people including a suite of education resources, iParent and Young & eSafe.

- Targeted presentations and workshops to groups and organisations such as mental health and social workers, sporting organisations and law enforcement who are positioned to influence and to assist others to identify, assess and self-manage online risks.

- Online safety initiatives for older Australians and women at risk of experiencing technology-facilitated abuse (and the front line workers who support them) through our Be Connected and eSafetyWomen initiatives respectively.

eSafety's online safety resources are informed by research, stakeholder engagement, and eSafety's learnings from investigating reports about cyberbullying, image-based abuse and illegal online content.

eSafety also encourages industry to take more responsibility for producing safer services in the first place through initiatives like Safety-by-Design which aim to embed protection for online users at the design stage of the product development process. This is meant to shift the responsibility for platform safety on the technology providers themselves, rather than placing the burden on users, or requiring Government intervention after the damage has been done. Four overarching principles underpin eSafety's vision for Safety-by-Design, including: platform responsibility, recognition and respect for user identity, user empowerment, and transparency and accountability.

[10] See s.15 of the *Enhancing Online Safety Act 2015* which prescribes the functions of the Commissioner.

Even with the best prevention programs, there will always be instances of troubling online content or behaviour that warrant government intervention to minimise harm. The Act and the Broadcasting Services Act 1992 (Cth) ('the BSA') recognise as much, with their respective statutory schemes to address serious cyberbullying targeting Australian children and offensive and illegal online content. Further, the government has proposed legislation to address the harms caused by the non-consensual sharing of intimate images.

The cyberbullying complaints scheme encourages a cooperative approach between eSafety and its social media partners. Under the scheme, complainants must first report child cyberbullying material to social media partners before eSafety can request or require removal of the material, and the strong working relationships eSafety has with its social media partners means eSafety has not needed to use its formal powers to date. This cooperative approach is also evident in eSafety's new initiative to combat image-based abuse, with many platforms voluntarily removing image-based abuse material in response to requests from eSafety.

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?

Yes. eSafety believes an express statement outlining Parliament's intended regulatory approach should be included in the Act.

Such a statement would enhance clarity, transparency and accountability. It would also provide a clear expectation to the public, industry, other regulators and stakeholders about the Commissioner's regulatory objectives, as well as the rationale underpinning the scope and extent of the Commissioner's functions and powers.

The statement should be closely tied to the Commissioner's functions and powers under sections 15 and 16 of the Act.

The statement should be drafted so that it establishes overarching principles and objectives for the Commissioner. How to uphold these principles and objectives should then be at the discretion and judgment of the Commissioner.

eSafety welcomes the opportunity to provide input into the development of the statement. Its understanding and experience of legislative, regulatory and operational matters under the Act, and how to most effectively work with technology companies, would be particularly helpful in both informing and shaping the statement.

While detailing the exact matters that should be included in the statement is beyond the scope of this submission, broadly speaking, eSafety would be interested in principles and objectives relating to:

- public interest considerations the Commissioner should have regard to in performing her functions and powers

- establishing a risk based, proportionate and gradated approach to regulation, compliance and enforcement
- ensuring online safety standards that are robust, reasonable and effective, and
- the coordination, advisory and leadership role the Commissioner plays across government and the broader online safety community in Australia.

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?

No, revisiting and extending the Basic Online Safety Requirements is required. eSafety believes that Australians' online safety would be enhanced if additional requirements were included in s.21 of the Act.

There is increasing consensus that online service providers have a duty to ensure that user safety is integrated into, and at the forefront of, the design, content and functionality of their services. This is called 'Safety-by-Design' and has become an area of focus for eSafety, which is consulting with industry, community and academics to share ideas and develop future approaches. Increasing the basic online safety requirements for social media services is also a recommendation of the Senate Cyberbullying Inquiry.[11]

Expansion of the basic online safety rules is required to keep pace with the evolution of technology and the way that young Australians have embraced online connectivity. For example, our research report, '*State of Play – Youth, Kids and Digital Dangers',* finds that Australian children aged 8 – 17 years are already active users of social media, with or without the consent of their parents or guardians, and that they are sharing personal information online. Our research has also found that 33% of young people on social media experience unwanted contact and content.

To strengthen protections for users of online service providers, the existing basic online safety requirements could be expanded to include:

- risk management processes and impact assessments pre-deployment
- more clarity in user-safety policies, procedures and processes with proof of platform enforcement
- more robust user-safety settings and safety measures incorporated into the platform or service
- tools, advice, resources and guidance on user-safety and digital wellbeing in-app or in-platform
- clear, plain-English and transparent community standards and terms of service

[11] Senate Legal and Constitutional Affairs References Committee, Report, 'Adequacy of existing offences in the Commonwealth Criminal Code and of state and territory criminal laws to capture cyberbullying', March 2018, Recommendation 6

- transparent and meaningful data on safety metrics that demonstrates accountability and progress

There is also a need to expand the basic online safety requirements beyond social media services to a wider range of platforms where various forms of online abuse are already taking place. We know from our research and complaints coming into our office that any online platforms that facilitate social interaction provide an opportunity for cyberbullying, cyber abuse and online grooming. These could include popular messaging apps like WhatsApp and Skype and a range of gaming platforms, some of which have expressed interest in becoming Tier 1 services if permitted. Apps stores like the Google Play Store, Apple iTunes Store and Microsoft Store serve as valuable choke points for ensuring that online apps are age-appropriate and properly rated and should arguably have more responsibility under the online safety scheme.

Greater uptake of the basic online safety requirements would enable eSafety to be able to act on user safety and online content across the increasingly diverse range of platforms and services that Australian children are using, and are experiencing abuse on. We should also seek to future-proof the next iteration of the legislation so that emerging technologies and platforms ranging from Internet of Things (IOT), robotics, artificial intelligence applications, and augmented and virtual reality platforms cannot be misused or facilitate abuse without repercussions.

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?

Yes. We know that approximately 1 in 5 Australian children are cyberbullied. While social media services should take primary responsibility for preventing and removing cyberbullying on their platforms, we serve as a safety net when serious cyberbullying is not taken down by a social media service so that the humiliation for the child does not persist and escalate. Since July 2015, eSafety has received and assessed over 900 cyberbullying complaints under the cyberbullying complaints scheme.

The complaints that come to us are often highly complex, rooted in school conflict and fall into the “grey area” – that is, on its face, it may not clearly contravene the platform’s terms of service. It is these types of cyberbullying where detailed examination of the material and context is most needed and often unable to be provided by the platform. We help to correct the inherent imbalance that exists between the social media site and the young user when the abusive material is not taken down, and there is no right of appeal. Safety has been able to effect the rapid removal of serious cyberbullying material through its relationships and escalation pathways with social media services under the two tier scheme. Serious cyberbullying material is commonly able to be removed within a few hours.

While the most effective measure to address cyberbullying is prevention, it is important to remember that this is a social and behavioural issue playing out online that has existed since time immemorial. Face-to-face bullying is still more prevalent than cyberbullying and full scale cultural change will take time. Given these realities, we know the most beneficial thing we can do as a Government entity is to provide early intervention services through

removal of the violating content, which will give relief and minimise harm to the target of the cyberbullying. In addition to helping to remove material, we provide practical guidance to children and their parents and carers to help them deal with cyberbullying and to protect themselves online. We also refer children to support services like Kids Helpline and have arrangements in place that enable us to conduct a "warm transfer" to Kids Helpline counsellors when needed.

We know that cyberbullying cannot be addressed by any single response, but must be combatted through a multi-layered approach involving partnerships between government, industry, parents, carers and schools. This is precisely why we also work with the victims, their parents or carers and the broader school community to help address the roots of the social conflict that may have precipitated the cyberbullying, and schools have told us that once we have been involved, the bullying – in all of its forms – tends to dissipate.

The impact that eSafety can make to the lives of cyberbullying victims is often highlighted through the feedback received from complainants. For example, the principal of a school attended by cyberbullying victims recently provided her appreciation of the support and help eSafety was able to give to the family and was thankful that a service like the cyberbullying complaints scheme existed. The Senate Cyberbullying Inquiry was likewise strongly supportive of both the role of eSafety and the cyberbullying complaints scheme specifically.[12]

The success of the cyberbullying complaints scheme is dependent on Australians knowing about it and the support that eSafety can provide. eSafety has driven a range of outreach efforts including the eSafety National Day of Action ('NDA') against Bullying and Violence activities and Safer Internet Day ('SID'), which reached over 42,000 and 55,000 students respectively through virtual classrooms. Despite the year-on-year growth in the number of cyberbullying complaints that have been received, eSafety is still very new and public awareness of it is still growing.

There is a need to increase national awareness of the cyberbullying complaints scheme as well as greater research into help-seeking behaviours and other ways to encourage young people to report cyberbullying. The need to increase awareness was a finding of the Senate Cyberbullying Inquiry which recommended that the Government better promote the role of eSafety and the cyberbullying complaints scheme.[13]

We have the capacity and the will to help more young people in the face of cyberbullying and will keep up our awareness activities in the hope that more children, and those supporting them, will continue reporting to eSafety.

[12] Senate Legal and Constitutional Affairs References Committee, Report, 'Adequacy of existing offences in the Commonwealth Criminal Code and of state and territory criminal laws to capture cyberbullying', March 2018, 5.16

[13] Senate Legal and Constitutional Affairs References Committee, Report, 'Adequacy of existing offences in the Commonwealth Criminal Code and of state and territory criminal laws to capture cyberbullying', March 2018, Recommendation 6

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?

No. The fact that eSafety has not needed to use its statutory powers under the two-tier scheme does not mean they have not been valuable or are unnecessary (the end-user notice scheme is discussed in the response to question 5(d)). It is the preference of eSafety to work informally and flexibly with social media services where possible to ensure cyberbullying material is taken down as quickly as possible. In this way, the cyberbullying complaints is largely already working as a cooperative model between the Government and industry. However, the powers available to eSafety to compel social media services to remove serious cyberbullying material provides a critical safety net and drives social media services to take cyberbullying as seriously as the Government and the Australian community expects them to. By supporting young people to effect the removal of cyberbullying material, these powers have helped to correct the inherent power unbalance between social media platforms and the Australian children who use them. And, while the cooperative approach has worked so far, there is no question that prospect of regulatory intervention has encouraged both responsiveness and action for the tier scheme members.

While the number of social media services who have chosen to voluntarily join Tier 1 continues to grow, the Minister has nevertheless needed to use his powers to declare Tier 2 social media services, including some of the largest social media services in the world. There is no way to predict the extent to which Tier 2 social media services are likely to be expanded over time. In future this could include social media services who are resistant to removing cyberbullying material. Holding regulatory powers in abeyance to ensure compliance with written notices is appropriate. The volume, severity and complexity of cyberbullying complaints is increasing and there is a strong possibility that eSafety will need to issue a social media service or end-user notice or take enforcement action in the future.

eSafety does not consider that an industry-based approach, particularly self-regulation without any regulatory oversight, would be more effective than the current cyberbullying complaints scheme or would provide stronger protection to Australian children. The cyberbullying complaints scheme has been designed to serve as a safety net and does not prevent social media services from strengthening individual or collective approaches to dealing with cyberbullying and online abuse. Rather, the cyberbullying complaints scheme complements and encourages better industry-based approaches given that that complainants must first report cyberbullying to a social media service and provide them with a 48 hour window to remove the material.

From eSafety's perspective, potential risks with industry codes (without oversight) or self-regulation include:

- There has been little transparency surrounding the measures that many social media services put into place to deal with cyberbullying, including the number and types of complaints they receive and how they are resolved (the Senate Cyberbullying Committee recommended that the Government consider requiring

social media platforms to publish relevant data, including data on user complaints and the platforms' responses[14])

- There is a power imbalance between users and social media services and users often may not always have visibility of decisions to remove (or not remove) content or be provided an opportunity to appeal

- Most social media services are based overseas with minimal Australian presence or an understanding of the specific cultures, context or community standards that may help to understand cyberbullying material in an Australian context

- There has been a proliferation of social media services and platforms in recent years and many newer or niche apps may be unwilling to conform to any voluntary code or industry self-regulation

- As previously discussed, most of the cases that come into eSafety are highly complex, rooted in school conflict and fall into a “grey area” that, on its face, may not clearly contravene the platform’s terms of service. This is where the Government plays a vital role of providing that additional context to the service, by advocating on behalf of the child, and spurring the company into takedown action.

Given the over 900 cyberbullying complaints that have been received, eSafety does not consider that there is sufficient evidence to justify removing or reducing regulation and moving to an industry-based approach. This approach would also be inconsistent with the findings of the Senate Cyberbullying Inquiry which recommended that the Government place and maintain regulatory pressure on social media platforms to prevent and quickly respond to cyberbullying material on their platforms, including through the use of significant financial penalties.[15]

There are arguments to consider reducing the time given to social media services to resolve cyberbullying complaints from 48 hours to 24 hours. Given the increasing volume and severity of cyberbullying complaints on victims, a tighter window would help to significantly reduce the harm and impact of cyberbullying material remaining on the internet. Given the improvements to reporting, flagging and moderation systems that many social media services have implemented since the Act came into force, eSafety does not consider that a 24 hour window is unreasonable.

eSafety believes that the current system already provides an effective and practical level of co-regulation that combines the benefits of industry innovation and responsiveness together with regulatory oversight and an escalation pathway for Australian children to ensure that cyberbullying complaints are appropriately considered and actioned. As noted in the Explanatory Memorandum to the Enhancing Online Safety for Children Bill 2014, social media services can be expected to benefit by being able to rely upon a proper assessment by an independent authority into the circumstances of particular cases. However, eSafety encourages the development of codes of practices and the

[14] Senate Legal and Constitutional Affairs References Committee, Report, ‘Adequacy of existing offences in the Commonwealth Criminal Code and of state and territory criminal laws to capture cyberbullying’, March 2018, Recommendation 6

[15] Senate Legal and Constitutional Affairs References Committee, Report, ‘Adequacy of existing offences in the Commonwealth Criminal Code and of state and territory criminal laws to capture cyberbullying’, March 2018, Recommendation 6

strengthening of industry-based interventions that would help to improve collaboration between industry and Government against cyberbullying.

Question 5(d):

Does the End-User Notice Scheme provide an appropriate safety net if industry cooperation fails?

No. eSafety has not considered that the issuing of an end-user notice has been appropriate or necessary in the circumstances of a complaint it has received to-date. While end-user notices can play a role to directly target the behaviours that drive cyberbullying, the issuing of an end-user notice is a very significant action to take and a power that should be taken with a high degree of discretion and care and only in the most serious cases. There are often also significant practical barriers to the issuing of an end-user notice. However, eSafety does not consider that these challenges warrant the repeal of, or significant changes to, the end-user notice scheme at this stage. More time is needed to test the effectiveness of end-user notices before they could be relied upon to provide an appropriate safety net to any potential future industry-based approach.

Cyberbullying mostly occurs between children, meaning that end-users (a person who posts cyberbullying material targeted at an Australian child) are generally children themselves. End-user notices can require a person to take a number of actions and failure to comply may result in a formal warning or injunction action. eSafety is acutely aware of the psychological and emotional impact a notice could have on a child and considers that the use of an end-user notice should be discretionary and proportionate to the circumstances. This is highlighted by research that indicates that people who engage in cyberbullying may be victims of cyberbullying themselves, may suffer mental health issues and may be at heightened risk of suicide.

Cyberbullying incidents are often highly complex and the facts difficult to ascertain. Complaints that eSafety receive may often only contain limited information and may not provide the wider context of the deep inter-personal conflict that can underpin cyberbullying. For example, there is a risk that a cyberbullying complaint potentially only illuminates one side of a conflict where both parties have cyberbullied each other. eSafety has limited investigative powers and in these circumstances may lack the necessary information to determine whether an end-user notice would be appropriate. A better resolution may be provided through the two-tier scheme, which focusses on the cyberbullying material itself rather than the people involved, and working cooperatively through a school to help address the underlying behaviour directly. In our experience, cyberbullying behaviour stops and rarely continues after our intervention in a matter.

A practical challenge to the end-user notice scheme is that it can sometimes be difficult or impossible to identify the end-user. Cyberbullying material can be posted anonymously or through fake or impersonated accounts and eSafety does not have the powers to compel social media services to provide information that could help to identify end-users. In a small number of matters, eSafety has requested user information from social media services to assist with assessing a complaint but has not been successful. This issue was considered by the Senate Cyberbullying Inquiry which recommended that consideration be given to improving the ability of eSafety to work with the Australian Federal Police to

access social media account and other relevant data to improve its ability to apply the end user notice scheme.[16]

These risks and challenges demonstrate that an end-user notice will not be an appropriate action to take in most cases and should be reserved for the most serious cases (eg. an end-user notice could be used against an identified teenager engaging in sustained cyberbullying, following an assessment of risks, or against an adult). eSafety does not consider that these challenges are fatal to the end-user notice scheme and is not necessarily seeking reform at this time. However, these challenges mean that the end-user notice scheme—at least in its current form—would not be an effective safety net to any potential industry-based approach.

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?

Overall, yes, eSafety considers that the definition of serious cyberbullying in paragraph 5(1)(b) as 'material [that] would be likely to have the effect on the Australian child of seriously threatening, seriously intimidating, seriously harassing or seriously humiliating the Australian child' is adequate and sufficiently broad to cover the range of cyberbullying material that young Australians are experiencing. The only caveat is explored in this submission's response to Question 5(g) about other types of harmful online content.

On the other hand, eSafety believes that s.5(1)(a) of the Act is inadequate for capturing the main sources of cyberbullying material. Section 5(1)(a) specifies that the material must be provided on a 'social media service or relevant electronic service'. However, the definitions of 'social media service' (s.9) and 'relevant electronic service' ('RES') (s.4) under the Act are narrow and not mutually exclusive. The definitions have caused confusion among stakeholders as to which services are captured by each definition.

Since the two-tier scheme and eSafety's enforcement powers in Part 6 of the Act only applies to social media services, some platforms may contend that they are not captured by eSafety's regulatory powers. That is, the lack of distinction between a social media service and a RES under the Act means many platforms can successfully argue that they are an RES, rather than a social media service. Narrow definitions and the blurring of boundaries therefore presents an obvious loophole that could compromise any future enforcement action if challenged.

The proliferation of communications technologies and platforms means that the distinctions between a social media services and a RES are becoming more and more blurred. For example, communications apps like Facebook Messenger, WhatsApp, and Skype, together with numerous online gaming services, facilitate high degrees of social interaction and the sharing of communications and materials which can include cyberbullying. The app environment is highly dynamic and since eSafety was created, Sarahah and other anonymous messaging apps have been developed and have achieved

[16] Senate Legal and Constitutional Affairs References Committee, Report, 'Adequacy of existing offences in the Commonwealth Criminal Code and of state and territory criminal laws to capture cyberbullying', March 2018, Recommendation 6

global popularity and notoriety for the callous and untraceable taunts to peers they have enabled.

Consideration should be given to changing or clarifying the definitions of a social media service or RES so that eSafety can respond more flexibility to the kinds of platforms that children are using and may be using to send cyberbullying material. To assist victims of cyberbullying, it is important for eSafety to be able to act on material across the spectrum of digital devices, services and platforms that enable interactivity. eSafety suggests that the problem may be rectified by replacing social media services and RES with a single term, such as 'interactive services and platforms'. This would provide eSafety with better recourse to assist the growing number of young children who use online end-to-end services.

This view is supported by the findings of the Senate Cyberbullying Inquiry which accepted that the existing definitions may not adequately capture all platforms on which cyberbullying occurs and recommended amending the definitions of 'social media service' and 'relevant electronic service' to expand the scope of the two-tier scheme.[17]

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?

No. It is not clear what benefit could be gained by removing the definition of cyberbullying from the Act. The definition of cyberbullying in the legislation gives clarity about the Government's mission, sends a message to the community about harmful behaviours and provides regulatory certainty to social media platforms and other online services operating in Australia. As discussed in this submission's response to question 5(e), the existing definition is sufficiently broad to include a wide range of cyberbullying behaviours. While it is important for the definition of cyberbullying to evolve as community attitudes and expectations shift over time, the legislative process already provides the appropriate and transparent mechanism for achieving this. If the definition of cyberbullying is de-coupled from the Act, it is not clear where it could more logically belong.

It is worth noting that the education sector plays a critical role in helping combat cyberbullying and are critical partners of ours at the national, state, territory and local levels. Specifically, we believe that the education sector is in a unique position to make significant progress in the fight against cyberbullying if they focus on two main areas – the curriculum and local remediation efforts in schools.

While the curriculum is crowded, eSafety believes that online safety skills need to be consistently taught, practiced and reinforced throughout the pre-K to 12 curriculum. Ideally, this would be in addition to the basic, online "do's" and "don'ts" parents and carers should all be practicing at home.

[17] Senate Legal and Constitutional Affairs References Committee, Report, 'Adequacy of existing offences in the Commonwealth Criminal Code and of state and territory criminal laws to capture cyberbullying', March 2018, Recommendation 6

The teaching of online safety skills should include the 4 R's of respect, resilience, responsibility and reasoning. This should take place consistently throughout a child's educational experience as they serve as critical values-based principles in the real world. To assist in this learning and program delivery, there are a range of evidence-based education resources developed by eSafety and currently available and mapped to the National Curriculum, as well as other resources.

In addition, we believe the states can make significant progress in the fight against cyberbullying through the allocation of staff to help students resolve online—and offline—conflict. Having staff on-the-ground to identify, surface and ultimately unravel and resolve this conflict is critical.

These school personnel may be counsellors or well-being coordinators that are already in-place or may be newly-designated "cyber safety school liaison officers." There are already schools in some states implementing this model at the local level, leveraging the resources and training offerings of eSafety, which has proven very effective.

eSafety supports the work of the COAG Education Council and is a key contributor and advisor to its cyberbullying work program. On 22 June 2018, the Commissioner gave a presentation to the Council where she spoke about the importance of strengthening Commonwealth and state and territory efforts to address the cultural and behavioural problems that underpin cyberbullying and to explore greater opportunities for eSafety to work in partnership with state and territory education sectors.

eSafety is continuing to work closely with the COAG Education Council and is contributing to work programs and review processes that are undertaken in the states and territories, such as current inquiry by the Queensland Anti-cyberbullying Taskforce. Given eSafety's clear role targeting cyberbullying, its national regulatory role, its coal-faced exposure to cyberbullying behavior that is occurring through the cyberbullying complaints scheme and its research function, eSafety is best placed to monitor changes in community attitudes around cyberbullying and to identify when the definition may need to be adjusted.

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?

Yes, expanding current arrangements should be considered. As discussed in the response to Question 5(e), eSafety considers that the existing definition of serious cyberbullying is adequate and sufficiently broad to cover the range of cyberbullying material that young Australians are experiencing. Many other kinds of harmful content are addressed through the Online Content Scheme and eSafety's work combatting cyber abuse and image-based abuse.

It is important for Government to remain vigilant about the potential impact of new and existing forms of online content and community attitudes around them. For example, Government could consider expanding the scope of Part 3 of the Act beyond cyberbullying to a wider range of online content that may be harmful for children, such as online grooming or incitement to (or encouragement of) suicide and other forms of self-harm. These behaviours, while often insidious or harmful, may not always take an obvious cyberbullying form. Expanding the cyberbullying complaints system to include a wider

range of cyber abuses would not only maintain eSafety's relevance by capturing the reality of young people's online experiences but also better assist eSafety's obligations under the Act. If Part 3 of the Act is broadened in such a way, care should be taken to avoid or minimise impact on existing or proposed laws and, where relevant, potential existing law enforcement activities.

Given the expanded remit of eSafety, Government could also consider expanding the cyberbullying complaints scheme to include cyberbullying targeting adults, as was recommended by the Senate Cyberbullying Inquiry[18]. Government would need to determine whether the same standard of 'serious cyberbullying' should be used and whether the scheme should be expanded to cover all Australian adults or limited to certain groups of vulnerable adults, however determined. However, expanding the cyberbullying complaints scheme to include adults would likely lead to a significantly higher volume of complaints from adults than are currently received from children and exceed eSafety's existing resources, a point that the Senate Cyberbullying Inquiry also acknowledged[19].

Already, we have received more than 300 cyber abuse complaints from adults since our remit was expanded. Moreover, the types of cyberbullying being reported to eSafety by adults is often more complex and longstanding than cyberbullying behavior between children. This means that they can be much more time and labor-intensive to assess and challenging to resolve. While we currently provide general guidance and support for adults experience cyber abuse, the absence of a formal framework or powers for investigating cyber abuse targeting adults significant limits what assistance we are able to provide.

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?

Yes, it is appropriate the Minister has this power. Under s.30 of the Act, the Minister may, by legislative instrument, declare that a social media service is a tier 2 service. The Minister may only do so if the Commissioner has recommended the making of the declaration. Section 31 provides a number of parameters for the Commissioner in making a recommendation, including that the Commissioner must be satisfied that the social media service is a large social media service or the social media service has requested the Commissioner to make the recommendation. The Commissioner must also consult the social media service before making any recommendation.

The Minister has to date declared four social media services to be Tier 2 services, Facebook, Instagram, Google+ and YouTube. Tier 2 services are subject to legally binding notices and penalties of up to $21,000 for non-compliance. While providing this power to the Commissioner could reduce the time it takes to declare a Tier 2 service, eSafety considers that it is appropriate for this power to remain with the Minister given the

[18] Senate Legal and Constitutional Affairs References Committee, Report, 'Adequacy of existing offences in the Commonwealth Criminal Code and of state and territory criminal laws to capture cyberbullying', March 2018, Recommendation 6

[19] Senate Legal and Constitutional Affairs References Committee, Report, 'Adequacy of existing offences in the Commonwealth Criminal Code and of state and territory criminal laws to capture cyberbullying', March 2018, 5.20

significance and regulatory impact of a social media service being declared a Tier 2 service.

Keeping this power with the Minister ensures that the highest degree of consideration is given to a decision to declare a social media service a Tier 2 service, given that both the Minister and Commissioner need to be supportive. Declarations made by legislative instrument also provide greater public accountability and transparency than an administrative decision of the Commissioner given that they are subject to Parliamentary disallowance.

Question 5(i):

Is the tiered system still the best approach? If not, are there other approaches that would be preferable?

Overall, yes. The main advantage of the current tiered system is that it provides an opportunity and incentive for social media services to work cooperatively with eSafety to effect the rapid removal of cyberbullying content. Unlike Tier 2 social media services, Tier 1 participants are not subject to any direct enforcement measures, although Tier 1 status may be revoked if there is repeated failure to comply with requests to remove material over a 12 month period. The tier system also ensures eSafety retains powers to take action against large social media services who are unable or unwilling to become a Tier 1 participants.

eSafety considers that the current tier system is effective, given the growing number of social media services that have chosen to become Tier 1 services, including Musical.ly, Roblox and Yubo in 2017-8, joining existing social media services like Snapchat and Twitter.

As discussed in the response to Question 5(e), eSafety considers that the definition of a social media service or RES should be changed or clarified so that a broader range of platforms and services can become Tier 1 or Tier 2 services. This would enable eSafety to respond more flexibility to the kinds of services and platforms that children are using and may be targeted by cyberbullying on.

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?

No. The scope and operation of each schedule lacks clarity. Reform to the Online Content Scheme since its inception has failed to create a clear distinction between the schedules, or to address duplication and apparent drafting errors.

The schedules are not drafted in a way that illustrates what each is for. While Schedule 5 largely addresses complaints about online provider rules and sets out code issues relevant to ISPs through Part 5, it also deals with matters that are more properly within the scope of Schedule 7 provisions relating to online content investigations.

For example, clause 40 of Schedule 5, and clause 69 of Schedule 7 both deal with referral of certain sufficiently serious online content to Australian police where the content has

been encountered through an investigation carried out under Division 2 of Part 3 of Schedule 7.

Duplication across the schedules also undermines their clarity of scope. For example, each schedule contains a provision that prescribes, in near identical terms, the way in which online content is to be assessed. That is, content must be assessed as if it were a film.

There are also weaknesses to the drafting of the schedules, resulting in errors and circular definitions. For example, sub-clause 40(4) of Schedule 5 refers to 'Recognised alternative access-prevention arrangements' that are relevant in cases where an industry code is registered that deals with certain matters. These matters are prescribed by clause 60 of Schedule 5. In sub-clause 60(2), the text refers to 'Designated alternative access-prevention arrangements'. The result is uncertainty around whether there are both recognised and designated alternative access-prevention arrangements, or a single class of alternative access-prevention arrangements.

Schedule 7 supplies a definition of 'Australian connection' at clause 3. That clause draws a distinction between the Australian connection of a content service, and the Australian connection of a hosting service. However, a content service's Australian connection can be made out if the content service hosts content in Australia. Under the definition of 'hosting service' under clause 4, a person can provide a hosting service if they provide hosted content. The result is circular definitions of both hosting and content service, in which either can be defined as the other.

These issues with the clarity of scope of each schedule creates confusion around any purported distinctions between them, while unnecessarily complicating administrative decision-making and the exercise of powers.

Question 6(b):

Is the Online Content Scheme effective in limiting the availability of prohibited content?

Yes. The Online Content Scheme is effective at liming the availability of Australian-hosted prohibited online content. Where prohibited material has an Australian connection – i.e. it is hosted or provided from Australia – the Commissioner has extensive powers of takedown established under Schedule 7 to the BSA. These powers provide for daily fines of up to $21,000 if an entity providing a hosting service refuses to comply with a final takedown notice. The BSA also prescribes formal warnings and civil penalty provisions, allowing for a range of effective enforcement measures to ensure Australia does not become a safe harbour for prohibited online content.

This is shown by the fact that, out of around 13,000 complaints from Australian residents handled by the Commissioner in 2017-2018, none concerned Australian-hosted prohibited content.

The overwhelming preponderance of prohibited online content that is the subject of complaints under the Online Content Scheme is hosted overseas. This fact creates regulatory challenges, as there is a jurisdictional limit to the reach of the Commissioner, who cannot issue take-down notices to overseas web hosts.

Our membership with the International Association of Internet Hotlines (INHOPE) is thus crucial to the ability of eSafety to take action against child sexual abuse material provided from overseas locations. In 2017, the INHOPE network exchanged 87,930 reports about child sexual abuse material, resolving to 259,016 identified images and videos. The vast majority of this material was taken down within 3 days.

The definition of 'prohibited content' in the BSA is problematic, however. It includes material, such as X 18+ content (showing explicit sexual activity between consenting adults) that is legal to sell by way of physical media in the ACT and NT. There is a lack of consistency in consequence between how online and offline media are regulated.

We recommend severing the link between the Online Content Scheme and the National Classification Scheme, with the latter reformed to concentrate on *harm* as a basis for determining whether content ought to be prohibited, rather than offence.

Question 6(c):

Is the Online Content Scheme providing an adequate safeguard for Australian children?

Overall, yes, but there may be constraints on the capacity of the Scheme to fulfil all aspects of its regulatory intent.

The BSA provides that it will function 'to protect children from exposure to internet content that is unsuitable for children'.

Currently, the BSA provides for this object to be satisfied via two mechanisms:

1. via takedown and removal of prohibited content hosted in Australia, thus limiting the potential exposure of such content to children, and

2. via the operation of the 'recognised alternative access prevention arrangement', which under relevant industry codes of practice is known as the Family Friendly Filter Scheme (FFF Scheme).

Under the FFF Scheme, vendors of filter products work with Australian ISPs to advertise the products to ISP customers. The products provide device-level protections against unwanted content, such as pornographic material. In independent testing commissioned by eSafety, an Australian benchmarking company showed that device level options were more effective at filtering content across a variety of categories than many network or appliance technologies.

Providing children with device level FFF Scheme-accredited filters, therefore, will likely be an effective means of safeguarding children from exposure to unsuitable material. However, this assumes that the FFF Scheme is itself an effective means of accrediting end-user device-level filters for consumer use. We understand that, while a number of filter vendors have commenced testing to obtain accreditation under the FFF Scheme, many have not met the bar.

This raises questions about whether the FFF Scheme can be regarded as capable of meeting the regulatory intent of the 'recognised alternative access prevention arrangement' prescribed in Schedule 5 to the BSA. Without a robust stable of filter vendors

providing products at various price-points, consumers cannot consider which product is most appropriate to their circumstances The result is little to no incentive for families to consider the FFF Scheme as an option when planning how to protect their family online, and little to no incentive for ISPs to promote the FFF Scheme to their customers.

Question 6(d):

Does the Online Content Scheme give the eSafety Commissioner appropriate powers to investigate and resolve complaints?

Overall, yes, but there is scope for clarification and strengthening.

The Commissioner's power to commence an investigation on her own initiative, and to investigate in any manner deemed fit, are both effective and appropriate powers to investigate and resolve complaints.

These powers are also effective and appropriate where the availability of child sexual abuse material is concerned. In situations in which an Australian resident reports child sexual abuse material, the powers contained in clauses 44 and 45 of Schedule 7 to the BSA are a productive way of ensuring that the fullest possible action can be taken against the availability of illegal and harmful content.

In the overwhelming majority of cases, this action will consist of referral to the INHOPE network.

One area which may benefit from clarification and/or strengthening is the power of the Commissioner to compel records from Australian designated content / hosting service providers. Such a power would be helpful in cases where a hosting service provider leases an IP address, and then supplies that IP address to downstream customers for the purpose of further hosting services.

Often, given the commercial chains involved in such relationships, the actual content service provider is several steps removed from the lessee of the IP address. In these cases, compelling information from the IP address lessee would assist to ensure that any takedown action was initiated by the Commissioner against the true content host, and not the lessee (who will often have no visibility into what is hosted at a website hosted at the leased IP address).

Question 7(a):

Are the enforcement tools available to the eSafety Commissioner appropriate?

Yes. The enforcement tools available to the Commissioner in respect of takedown action and breaches of online provider rules are appropriate.

The enforcement provisions consist of a graduated set of tools, from remedial directions and formal warnings, through to penalty amounts and civil penalties for non-compliance and injunctive action.

Neither under the ACMA, nor under the Commissioner, has there recently arisen a situation in which enforcement action has been warranted or initiated. Industry has complied with 100% of takedown notices issued under the Online Content Scheme, and complaints about online provider rules are rarely made.

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?

Yes. The takedown scheme has provided an effective means of ensuring that Australian-hosted prohibited content is removed, and removed permanently.

Ensuring the permanence of removal is the work done by provisions under Schedule 7 relating to anti-avoidance and the issuance of special take-down notices. However, it is arguable that the distinction between content takedown, service-cessation, and link-deletion is less relevant today than when Schedule 7 was first enacted.

A more accurate approach would entail noting that online content is, simply, online content, access to which might be subject to considerations about whether the content is harmful.

In this way, issues of non-compliance with the resultant regulatory regime would be dealt with via a single notice and takedown mechanism, instead of the three currently set out in Schedule 7 (i.e. content takedown, service cessation, and links deletion regimes).

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?

No, Schedule 5 does not provide for 'take-down' notices to be issued by the Commissioner against overseas-hosted prohibited or potential prohibited content.

Instead, clause 40 of Schedule 5 deals with the question of how action is to be taken in relation to a complaint about prohibited content hosted outside Australia.

Under that clause, the Commissioner must notify sufficiently serious online content to a member of an Australian police force, or another person or body under agreement with an Australian police commissioner.

All other overseas-hosted prohibited content is to be notified by the Commissioner under the clause to ISPs via the designated notification scheme. The designated notification scheme forms the basis of measures to inform the design and implementation of filter products offered under the FFFS Scheme via Internet industry codes of practice.

The clause functions effectively as a way of allowing the Commissioner to notify CSAM to members of INHOPE where the content is hosted in their jurisdiction.

This arrangement is established via an agreement between the Commissioner and the Commissioner of the Australian Federal Police. As noted elsewhere, the vast majority of CSAM notified to INHOPE by the Commissioner is removed within 1 – 3 days.

However, there are questions around the efficacy of the FFFS. These are dealt with elsewhere in this submission.

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?

No. The National Classification Scheme is not the most appropriate way to respond to current online content issues, and is inadequate to address emerging and future challenges.

These challenges include online content types that rely on fully immersive virtual reality environments, and increasingly dynamic and interactive modes of engagement. These modes of engagement include nascent forms of technology such as haptic suits, allowing for the simulation of physical sensations generated within virtual spaces.

One of the major difficulties is that the current assessment of online content under the BSA relies on the same criteria applicable to films. While early web content may have been roughly analogous with a film's elements, this is no longer the case. Today, content is dynamic, highly interactive and immersive, and often served to users in a way that caters to their preferences. An additional consideration is the vast volume of material accessible online that is user-generated content (UGC). Google estimates that 400 hours of new UGC content is uploaded to YouTube every minute.

While it may have been once appropriate to assess films embedded into web pages using the film classification criteria – given that, often, online film content is of a professional grade – it is arguably *not* appropriate to hold UGC against the same framework. After all, the framework was designed to assess commercial output delivered by professional studios. In designing a vehicle for regulating online content, it should not be assumed that UGC will bear any similarity to content created for a market of paying consumers.

In addition, by yoking the Online Content Scheme to the National Classification Scheme categories, changes in community attitudes cannot be reflected in regulatory practice. For example, the Guidelines for the Classification of Films establish that the X 18+ category

cannot accommodate content showing adults engaged in consensual fetish activities, such as bondage. The result is that such content must be refused classification.

Finally, reliance on the National Classification Scheme produces inconsistency between classification regimes. For example, while it is legal to sell or hire X 18+ media in the ACT and NT, it is unlawful to host such content in Australia.

This raises questions around what might substitute for the Classification Scheme as a rubric of assessment where complaints about online content are concerned. At present, the classification categories require decisions to be made by assessors from the perspective of what is likely to be offensive to the reasonable adult. For example, Refused Classification (RC) content includes content that offends against standards of morality and propriety; and content that consists of an offensive depiction of a child, whether or not engaged in sexual activity.

A better standard, and one that would allow the Online Content Scheme to be separated from classification policies and practices, would be to assess whether the content is *harmful*. Such an assessment might then act as a way of preventing access to content that is likely to *do* harm (for example, preventing children accessing violent and degrading online pornography), or preventing access to content production of which was harmful (for example, child sexual abuse material).

A harm standard would allow for faster assessments by the Commissioner about material that really concerns Australians. It would also sever the reliance on the Classification Board for final determinative decisions (prior to regulatory action) and ensure that user-generated content is assessed according to a measure that is consistent and fair.

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?

No. Currently, the eSafety Commissioner relies on the Classification Board in two main ways. The BSA requires the eSafety Commissioner to, from time to time, submit samples of content subject to a complaint to the Classification Board for classification. When this happens is at the discretion of the eSafety Commissioner.

However, the eSafety Commissioner *must* apply to the Classification Board for classification before final takedown action against Australian-hosted content can be taken.

This reliance by the Commissioner on the Classification Board for final determinative decisions about online content is outdated and inefficient. It does not recognise the degree of expertise held by the Commissioner where the assessment of online content is concerned.

Moreover, by relying on the Classification Board, the Commissioner --and the Australian taxpayer --incurs considerable monetary cost. Each routine application is charged at the rate of $550. Routine applications are completed in 28 days, whereas priority applications – which attract an additional fee of $420 – are concluded in five days.

These time-frames are too long, especially where illegal online content such as child sexual abuse and pro-terror material is concerned. In addition, the cost impact is too high,

and given the significant increase in complaint and investigation volumes in recent years, the potential budgetary impact on the Commissioner is considerable. Even supplying occasional samples of complaint content for classification would result in the expenditure of thousands of dollars each year.

Where assessment of online content is concerned, there is a far greater degree of experience within eSafety than within the Board. Officers conducting content investigations for the Commissioner receive training in age assessment from leading paediatric specialists, and regularly exchange information and experience with other INHOPE hotlines around the world.

This training contributes to classification assessments made by eSafety officers that are highly accurate, and capable of being made in minutes, not weeks.
The result is a far higher degree of confidence and accuracy in the analysis of – especially – illegal online content such as child sexual abuse material, and provided in far shorter timeframes, than is possible through the Board.

Questions 9(a) and 1(c)

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?
and
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?

Yes. There is merit in moving the functions of the Commissioner expressed throughout Schedules 5 and 7 into the Act. The benefit lies in creating a single source of enumerated functions which, when read together, would act as a comprehensive statement of the Commissioner's role.

Clear regulatory efficiencies would flow from this arrangement. For example, the collected functions would better signal to industry the ambit of the Commissioner's role. If like functions were grouped together, clarity of scope would be enhanced, while reducing confusion or uncertainty about how the Commissioner intends to regulate specific sections of the Internet industry.

It might also benefit comprehension if functions were arranged in a way that illustrates the complementary nature of the Commissioner's functions.

This would suggest that Schedules 5 and 7 should be synthesised into a single instrument and inserted into the Act as an additional Part.

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?

The Online Content Scheme

Yes, it is critical that the online safety regulatory framework is capable of addressing emerging issues and trends.

There is broad agreement internationally that there are three main approaches to the classification of emerging technology.

The first involves regulation supported by legislation that applies to the function of a specific product, rather than the underlying technology. The intent is to produce technology-neutral regulatory mechanisms.

The second allows for ex-post determinations of legality or illegality, which are often retroactively validated by judges based on criteria specified within legislation.

Thirdly, technology classifications can attempt to encompass all future technological developments within the widest possible envelope. An example is the *Children's Online Privacy Protection Rule* ('COPPA'), a US Federal regulation prohibiting unfair or deceptive practices in connection with the collection of personal information from and about children on the Internet. COPPA takes a highly expansive approach to defining 'Internet', including all hardware and software elements of relevant networks.

eSafety believes that the first option is likely to yield the greatest dividends for the design of a successor regulatory scheme to the Online Content Scheme.

Seeking to ground classification in functional aspects of the thing being regulated allows its current and emergent functions to be dynamically interpreted. The resulting framework might be then considered a 'living agreement', capable of accommodating both technological advances and evolutions in consumer preferences.

The cyberbullying scheme

To remain effective, eSafety must be able to quickly act on abuse material across the spectrum of interactive digital devices, services and platforms that enable cyber abuse and cyberbullying.

The Act permits eSafety to intervene in a wide variety of instances involving serious cyberbullying affecting an Australian child. However, there is uncertainty over whether certain online services that are capable of facilitating cyberbullying material might be considered a 'social media service' within the Act. These services include apps such as Whatsapp, and rich interactive gaming platforms.

If a service is not a 'social media service' within the meaning of the Act then eSafety is left with little recourse to assist affected persons given that the tier scheme – and the regulatory levers attached to it – applies solely to social media services.

There is merit in revisiting the notion of limiting the tier scheme to social media services. An alternative approach would be to broaden the scheme's operation to include a wider range of rich interactive services, including those provided by gaming platforms. As noted in our response to question 5(a), this could include applying a domestic regulatory framework to the classification of apps provided by services such as Apple's App Store and the Google Play Store.

Finally, the advent of augmented reality, virtual reality, the Internet of Things, encryption, distributed-ledger based systems and other developments, have the potential to radically transform the digital landscape. As such, no legislation should exclude the potential of these technologies.

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?

Yes, there are a number of options for regulating online content based on the approach taken by peer nations, however insufficient time has been provided for submissions to allow for a full and balanced analysis of their advantages and disadvantages.

There is no singular model for internet regulation. Regulators are currently fitting the internet into their existing regulatory framework, with each regulator considering the country's framework and regulating the internet to advance its own perceived needs and benefit.

However, equally, there is argument for the need to create new regulatory environments that reflect the novel and unprecedented challenges posed by dynamic and immersive online content.

Where the provision of online services and products tailored to younger customers is concerned, there is potential to regulate aspects of the design process. These regulations would ensure that developers are accountable for the technology, especially in the context of making their offerings safe for children.

Questions 10(a), (b), (c), (d), (e) and (f):

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?
and
The industry codes were made in 2005 and 2008. Have the Codes kept pace with changes in technology and consumer behaviour?
and
Have the industry codes encouraged the development of internet technologies and their application?
and
There are four separate codes, found in two separate documents. Would a combined, single code provide clarity and be easier to administer and enforce?
and
Do the industry codes reflect current community attitudes?
and
Is the Family Friendly Filter (FFF) scheme effective in protecting Australian families from prohibited content?

No. The codes registered under Schedules 5 and 7 are anachronistic, out of phase with current industry practices, and reflect consumer preferences that are no longer relevant. There is no evidence that they have fostered the development of new internet technologies.

Advice provided to us by industry is that they are unable to comply with the codes, as they deal with obsolete and redundant technologies and policies, such as those dealing with adult chat and mobile premium services. It should be noted that, even though no more than two codes are permitted under Schedule 5, three are contained within the *Codes for Industry Co-Regulation in Areas of Internet and Mobile Content.*

All of the codes registered under Schedules 5 and 7 were drafted in a pre-smartphone, pre-cloud computing, pre-integrated social media age. They do not recognise the considerable safety, behavioural and societal changes that have followed introduction of those technologies.

At present, codes registered under Schedules 5 and 7 are required to contain certain content due to prescriptive provisions in the schedules. Even if new codes were developed by sections of the ISP and content industries today, they would still be required to reflect the matters listed in clause 60 of Schedule 5 or clause 81 of Schedule 7.

It is arguably unhelpful to have one set of codes focus on ISPs (those registered under Schedule 5) and another code focus on segments of the content services industry, but only where those content services have an Australian connection (i.e. are Australian hosted). This removes social media services from consideration in an age where Australians receive the vast bulk of their news, information and entertainment via services such as Facebook, Twitter and YouTube.

The Commissioner should be able to identify areas of the Australian online industry – such as games developers, social media services, app developers, ISPs, web hosts, and so on

– and encourage relevant industry groups to develop differential and relevant codes of practice under a single set of principles enumerated within the new Part created by synthesising Schedules 5 and 7. Some of these principles may be drawn from the eSafety Commissioner's 'Safety-by-Design' framework.

Finally, where the industry-administered FFF Scheme is concerned, it has not been effecting in protecting Australian families from prohibited content. The scheme should be reconsidered and replaced by an evidence-informed approach to providing device-level protections to Australian families.

Such a scheme should be expressed within industry codes that follow reform to the BSA, and should continue to be the responsibility of the Australian Internet industry to oversee and administer.

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.

In concluding, eSafety reiterates the importance of ensuring the online safety regulatory framework is achieving its objective of keeping Australians safe online.

Guided by our four regulatory pillars of *Prevention*, *Protection*, *Partnerships* and *Promotion,* eSafety adopts a wide, proactive and whole of community preventive approach, which allows us to deliver comprehensive, compassionate and citizen focused services.

This is why eSafety has built a reputation, awareness and profile as the expert and authority on online safety in only three years.

Adopting the recommended changes to our regulatory framework outlined in this submission will ultimately enable eSafety to more effectively and efficiently create a safe, positive and empowering online experience for all Australians.