Report of the Statutory Review of the Enhancing Online Safety Act 2015 and the Review of Schedules 5 and 7 to the *Broadcasting Services Act 1992* (Online Content Scheme)

Lynelle Briggs AO

October 2018

Disclaimer

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

This report has been prepared by an independent reviewer and does not indicate the Commonwealth's commitment to a particular course of action. Additionally, any third party views or recommendations included in this report do not reflect the views of the Commonwealth, or indicate its commitment to a particular course of action.

Copyright

© Commonwealth of Australia 2018

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

- any third party material
- any material protected by a trademark, and
- any images and/or photographs.

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

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

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

Third party copyright

The author has made all reasonable efforts to clearly identify material where the copyright is owned by a third party. Permission may need to be obtained from third parties to re-use their material.

Attribution

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

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

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

Contents

lynellebriggsAO

Senator the Hon Mitch Fifield
Minister for Communications and the Arts
Parliament House
Canberra ACT 2600

Dear Minister

As the independent reviewer appointed to conduct concurrent reviews of the *Enhancing Online Safety Act 2015* and of Schedules 5 and 7 to the *Broadcasting Services Act 1992* (the Online Content Scheme), I am pleased to present you with my completed review report on online safety regulation and governance arrangements.

The review report concludes that, even though current regulatory arrangements have been effective, major reform is needed to strengthen the regulatory regime and bring it into line with community expectations. New legislation is recommended, alongside changes in governance arrangements.

In undertaking this review, I have taken into account the views expressed in submissions and feedback received from stakeholders.

Yours sincerely

Lynelle Briggs

Lynelle Briggs AO

31 October 2018

Executive summary

The online industry has expanded so rapidly in recent years that it permeates every aspect of our lives and is increasingly central to the economic and social development of society.

Governments the world over have sought to harness its benefits by enabling the online industry to develop relatively free from regulation. Yet it has become more and more apparent over time that the powerful position the industry has taken in our lives requires a level of regulation which ensures that those using its services are protected from harmful, illegal or dangerous postings, or prevented from posting and distributing such material.

In the wake of path-breaking Australian Government legislation in 1999[1], the Australian industry has implemented leading-edge systems for taking down inappropriate content. However, more recent technological developments and the increasingly global nature of the industry have now made it relatively easy for harmful and dangerous material to be posted and distributed from overseas into Australia and elsewhere. While many countries have put in place arrangements to try to address these disturbing trends, the rapid pace of technological developments, especially the spread of social media and associated user-generated content, and the agile and inventive practices of distributers of illegal and harmful material, have defied conventional systems of complaints-based reporting and compliance.

While it is apparent that efforts to develop community protections have delivered results, the online safety system remains fragmented and is relatively unco-ordinated. I found in these reviews that the current system of industry co-regulation is insufficient to address the threats of harm, and that the legislation governing the system is in need of overhaul. The time has passed for further incremental change to legislation and industry practice. Major change is required.

The practice to date has largely been one of retrofitting child protection safeguards into online services and products after harm emerges, or the damage is done. It is much more effective to protect users upfront. The change required to establish a more fit for purpose, proactive regulatory regime will necessarily involve increased levels of black letter law.

I found in these reviews that the existing out-of-date and inconsistent legislation should be replaced by a new Online Safety Act and a new single code of industry practice. The new legislation will need to be clear in its intent. It should target what the online industry does rather than how they do it. It will need to be technology and device neutral—embracing all relevant platforms, services, distribution access mechanisms and devices and the future state of online and digital communication as far as is possible.

The proposed new legislation will need to guarantee that the online industry goes beyond simple compliance with minimum safety standards and should establish a much higher new benchmark standard with which all industry must comply.

The legislation should require industry to build online safety into its design arrangements *and* to proactively patrol, detect and remove harmful or illegal content at its source from their platforms, through the application of technology and greater human intervention. These proposed changes will need to be supported by a tougher and more interventionist enforcement regime involving law enforcement and the eSafety Commissioner working in partnership to collect information and data, detect misconduct, report compliance, and penalise wrongdoing.

[1] The *Broadcasting Services Amendment (Online Services) Act 1999* that introduced Schedule 5 into the *Broadcasting Services Act 1992*.

I found in these reviews that if online safety is to be effective, it should be recognised as a joint responsibility between industry, government and the community, with each having discrete roles to play. The rapid speed of adoption, spread of technology and burgeoning online industry and digital economy has meant that everyone working in the online safety field has been so busy just trying to manage the challenge of online safety, that they haven't had the time or space to sit back and reflect on what the core components of a national online safety strategy might be and who should be responsible for them, much less what an overarching policy might cover.

This has meant that, despite the many wonderful efforts of all the stakeholders working in the field to protect against and prevent online harm, the system remains fragmented, is difficult to understand and can be challenging to negotiate for those in need of help. In this, of all areas, arrangements and responsibilities need to be clear so that action can be quick and purposeful.

I have therefore recommended that:

- the Government's online safety policy be set out in new legislation that establishes a more proactive regulatory regime—the Online Safety Act;
- a new National Online Safety Plan be developed;
- mechanisms be put in place to correct for shortfalls in the effectiveness of the system;
- an eSafety Advisory Committee involving key stakeholders be established to meet at least quarterly to inform decisions, address duplication and overlaps, and propose online safety priorities and implementation strategy; and
- the eSafety Commissioner be the focal point for online safety nationally and for the regulation and co-ordination of online safety arrangements.

The current eSafety Commissioner, Julie Inman Grant, has been instrumental in driving change and raising the profile of online safety with industry and the wider Australian and international community. She has been very successful in the role, and has built on the success of the inaugural Children's eSafety Commissioner, Alastair MacGibbon.

However, there are a number of constraints which limit her effectiveness, principal among these being the governance arrangements surrounding her work. As part of possible transition arrangements towards a standalone online safety entity, I have proposed that the eSafety Commissioner and her Office be moved out of the Australian Communications and Media Authority and into the Department of Communications and the Arts, where the Department and the eSafety Commissioner could jointly work on policy, strategy and relationships. This will free the eSafety Commissioner up to work with industry to develop and implement the proposed new arrangements, and should enable her to give sharper focus to priority areas of online safety, such as more effective planning, education, research, prevention and behavioural change arrangements.

In such a dynamic environment, it is important to understand that no system of regulation can remain entirely effective in blocking and taking down harmful material. Industry and government need to be continually vigilant. They should keep innovating and taking action to address new online abuse and threat mechanisms as they arise.

Introduction

I was appointed in June 2018 by the Minister for Communications, Senator the Hon Mitch Fifield, to conduct two independent reviews of Australia's online safety legislation to ensure that it remains effective and relevant in protecting all Australians online. The Minister provided the following terms of reference for the reviews and sought completion of the reviews in the latter half of 2018.

Terms of Reference

Statutory Review of the *Enhancing Online Safety Act 2015*

The terms of reference of the statutory review of the *Enhancing Online Safety Act 2015* require a review of the following matters:

- the operation of the Act and the legislative rules;
- whether the Act or the legislative rules should be amended; and
- whether a delegation should be made under subsection 64 (1) of the Act.

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

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

Schedules 5 and 7 to the *Broadcasting Services Act 1992*

The review of Schedules 5 and 7 to the *Broadcasting Services Act 1992* (online content scheme) will examine the operation of the online content scheme, including:

- the relevance and effectiveness of the online content scheme in the context of the contemporary communications environment and modern consumption patterns of online media and services;
- the scope of regulation, including whether the online content scheme's link to the National Classification Scheme categories is still effective;
- the most effective balance of tools available for dealing with prohibited online content, including legislation, co-regulatory schemes, self-regulatory schemes and technical protections; and
- an assessment of other regimes, including international models, in dealing with prohibited content that is hosted overseas.

The review of the *Enhancing Online Safety Act 2015* must be tabled in Parliament within 15 sitting days after the completion of the report.

Process

The Department of Communications and the Arts (the Department) released a discussion paper in June 2018 which provided the basis for valuable input from industry, non-government organisations (NGOs) and individuals through submissions to the reviews. In addition to these submissions, I spoke to many people and organisations to garner their views and inform my recommendations. I would like to express my deep appreciation for their efforts to assist me in the reviews.

Because much of my work has involved overlapping issues and content between the two Acts, I have presented a single report covering both reviews for Ministerial and Parliamentary consideration, starting with the online content scheme schedules in the *Broadcasting Services Act*, then moving to issues relating to the *Enhancing Online Safety Act*, including the recent amendments to that Act made by the *Enhancing Online Safety (Non-consensual Sharing of Intimate Images) Act 2018*.

However, some of the content and commentary in one review is equally applicable to the other review, so there is necessarily some overlap, and I have opted to cover governance, regulation and legislation separately to manage the material more effectively. Nevertheless, this report should be read as one narrative with one set of recommendations.

I was generously supported in the reviews by officials from the Department. I would like to convey a special thanks to Mike Mrdak AO, Richard Eccles, Carolyn Patteson, Lynne Thompson, Ruvani Panagoda, Jonina Rivera, Vicki Buchbach and Catherine To.

Background

The Internet and the Digital Environment

The internet is a global collection of networks that connect together in many different ways to form the single entity of the internet. The internet works because open standards allow each network to connect to every other network. These open standards make it possible for anyone to create content, offer services and sell products without permission from a central authority.

There are some core standards for the internet that make it work, in particular the use of internet coding identifiers that can detect devices and allow information to be sent around the world. There is an internet hierarchy of internet provider addresses (servers), with domain names on those servers (which are underpinned by a unique number and a unique address), and sitting under them are uniform resource locators (URLs)), which specify the URL's location on a particular computer network and provide a mechanism for retrieving information from it within each of the domains.

Creative developers continue to extend the range of information sharing forms and options on the internet, and this has been facilitated by the movement from analog to digital and improvements in data compression, including digitisation. Along with these changes, we have seen the development of the digital environment, which is an integrated communications environment where electronic and digital devices are the tools which enable communication and manage the content and activities within it. A major component of the digital environment is the comprehensive presence within the internet of websites, cloud servers, search engines, social media outlets, mobile applications, and audio, video and other web-based resources.

Digital social environments are predominantly social networking sites, most of which need one central server to distribute information to members. Immersive digital environments create an artificial, all-encompassing sensory and virtual world where users can enter and share content or exchange ideas, do business, socialize or play games, and interact in real-time with other users or players dispersed around the globe. In line with our insatiable appetite for online content, available anywhere, anytime, and on any device of our choosing, Australians are experiencing a shift from primary engagement with the physical to a mutual reliance on the virtual[2].

The online environment has become an increasingly immersive and integrated part of our day. We rely on the online world to work, socialize, access and share information, and be entertained whenever and wherever we like. The result is a digital world that permeates nearly every aspect of our lives.

Even though there are some major players operating in this digital world, nobody owns it. It is the free and immediate flow of information that has made the internet so successful and so appealing to so many people around the world, and so effective in revolutionizing how economies and societies work.

The provision of such a free flow of information has enabled players in the internet industry to argue persuasively for it to operate in an environment relatively free from government regulation and, in turn, this has provided a new world economy with unparalleled access to information for users across the world as well as considerable commercial returns to industry players.

The free flow of information argument has also seen responsibility for the control of content firmly placed in the hands of individual users, who it is argued have the personal freedom to watch, participate in, share, ignore, or take down content. As a result, attempts to regulate to constrain the free flow of information on the internet have generally been met with opposition from companies directly and indirectly through their users, who have concerns about their potential loss of access, censorship and personal freedoms, and about constraints on the size and reach of the internet and on business and trade.

Australia has largely accepted these internet norms.

The trouble is that the world is not a benign place and the internet has not always been a force for good. In fact, it has facilitated bad behavior, manipulation and wrong doing on an unprecedented and previously unimaginable global scale in peacetime. In the words of the eSafety Commissioner:

> *"…there is an internet of infinite knowledge, unlimited discovery, an online world of enlightenment and ever-expanding horizons. But sadly, there is also a web of fear and of threats, of darkness and dark arts, of crime and exploitation."*

At an individual level, the explosion of user generated content and social media applications has raised awareness and heightened concerns in the community about the harm that can be done and the potential dangers for the innocent and the vulnerable in the online world. As an indication of these impacts, the Royal Melbourne Institute of Technology University found in May 2017 that 1 in 5 Australians, 1 in 2 Australians with a disability and 1 in 2 Indigenous Australians have experienced non-consensual sharing of images[3].

[2] Postmodernbible.blogs.com illustrates this.

[3] Dr N Henry, Dr A Powell and Dr A Flynn, *Not just 'revenge pornography': Australians' experiences of image-based abuse—A summary report* (May 2017), page 7, www.rmit.edu.au/content/dam/rmit/documents/college-of-design-and-social-context/schools/global-urban-and-social-studies/revenge.porn.report.2017.pdf.

The Office of the eSafety Commissioner (eSafety Office) advises that 1 in 5 Australian children are cyber-bullied[4] and that 1 in 10 Australian adults has had an intimate image shared without their consent. The eSafety Office produces a series of research papers, which show, inter alia, that in the 12 months to June 2017 almost 1 in 3 teenagers aged 14-17 had some experience with sexting and 42% of teens were contacted online by, or sent material from, someone they did not know. The eSafety Office's social cohesion research with the Department of Education and Training found that 57% of 12–17 year olds had seen real violence online that disturbed them and 56% had seen or heard racist comments online. One third of surveyed young Australians had seen videos or images that promote terrorism[5].

These Australian statistics are deeply disturbing. This is why effective and efficient oversight of the digital environment is so important, and why attitudes towards regulation are changing to enable these threats to be dealt with appropriately and consistently.

Submissions to the Reviews

The Department received 27 submissions to the reviews from a range of government, industry and non-government stakeholders. Those submissions are generally available[6] on the Department's website at **www.communications.gov.au/have-your-say/reviews-enhancing-online-safety-act-2015-and-online-content-scheme**, and provide a wealth of information and ideas about the way forward. They provide the basis for many of the recommendations in this report.

The key points raised in submissions in relation to the *Enhancing Online Safety Act 2015* were:

- There was broad support for the work of the eSafety Office from community and government agencies. However, industry stakeholders would like to see a stronger focus on education and awareness raising and behavioural change.
- In addition to the status quo, two governance models were proposed by the ACMA:
  - A standalone agency which is an 'Accountable Authority' under the PGPA Act; and
  - Full-time member or 'Associate Member' of the ACMA—would see online safety functions incorporated into the Authority, but maintain the public profile and leadership and organisational focus of the Office.
- There are many players in the field, so stakeholders would like to see better coordination of online safety efforts, less duplication of services and better leveraging of limited resources.
- The cyber-bullying complaints scheme is considered to be an appropriate safety net for users. The majority of submitters saw no justification for reducing regulation and moving to an industry-based approach.
- There was support for the expansion of the cyber-bullying scheme to adults.
- Community stakeholders believe the eSafety Commissioner should do more to compel industry to deliver on their responsibilities (e.g. through industry standards and codes of practice).
- The basic online safety requirements should be extended to a wider range of platforms and services and expanded to include more stringent requirements.
- Definitions of 'social media service' and 'relevant electronic service' should be future-proofed so that emerging technologies are captured.
- A full evaluation of the voluntary certification scheme for online safety program providers is timely.

[4] The most common forms of cyber-bullying are social exclusion, name calling, and the spreading of malicious lies and rumours.

[5] eSafety Office research overview, www.esafety.gov.au/education-resources/iparent/online-hate-infographic.

[6] A couple of those submissions contained confidential personal information and have not been uploaded on to the website nor are they available publicly.

Key points raised in submissions in relation to the online content scheme were*:*

- The majority of stakeholders who commented supported both moving Schedules 5 and 7 out of the *Broadcasting Services Act* and updating the online content scheme, resulting in:
  - a single piece of legislation relating to online services and content contained within the *Enhancing Online Safety Act*;
  - a single notice and take-down mechanism;
  - less prescriptive legislation with operational matters dealt with in a code; and
  - a technology/platform-neutral approach.
- Stakeholders agreed that the co-regulatory approach is working and remains the most effective and efficient approach to online safety.
- A number of industry stakeholders feel that using internet blocking to address illegal content or activities is generally inefficient, often ineffective and can cause unintended damage to internet users.
- Content hosts and content providers should exercise responsibility for content within their control in a manner consistent with the code.
- Industry and the eSafety Commissioner should take a more proactive approach and invest more in AI and machine learning to prevent illegal or anti-social content rather than relying on the community to report it.

Review of the Online Content Scheme

Australia was one of the first countries to appreciate the threat to child safety afforded by the internet through excellent early work by then Australian Broadcasting Authority (ABA)[7], which led to amendments to the *Broadcasting Services Act* in 1999 that established the legislative framework for online content co-regulation in Australia.

The upshot was to extend the co-regulatory system for broadcasting to online content, with Australian content assessed and taken down if found to be non-compliant with national classification requirements.

The co-regulatory system works by placing constraints on the types of online content that can be hosted or provided by internet service providers and content service providers, and providing a mechanism for users to complain to industry or government about prohibited or potentially prohibited content[8]. The sorts of prohibited content the co-regulatory system seeks to constrain are illegal material such as child sexual abuse material, extremely violent and disturbing pornography, extremist propaganda, incitement to terrorism, and games that victimise and abuse children or encourage illegal activity. It also seeks to restrict access to content that may be suitable for adults, but not children, such as R18+ content containing violence, drug use, nudity or realistically simulated sex and MA15+ content on certain mobile premium services.

[7] Which in 2005 combined with the Australian Communications Authority to become the Australian Communications and Media Authority.

[8] ‘Prohibited content’ is content that has been classified by the Classification Board as X 18+ or RC and, in some cases, content classified R 18+ or MA 15+ where the content is not subject to a ‘restricted access system’. Content is ‘potential prohibited content’ if the content has not been classified by the Classification Board and, if it were to be classified, there is a substantial likelihood that it would be prohibited content.

The co-regulatory system is supported by industry codes. Under these industry codes, commercial content providers and certain mobile content services assess some content in advance of uploading and assess uploaded content in response to complaints, and then apply the appropriate measures to manage end-users' access, which may involve take-down (including link and service deletion), blocking technology to prevent distribution, or access controls, such as restricted access systems like PINs and credit card age verification. The system also provides for a user-driven complaints-based mechanism at the internet service provider level. The codes also require industry to respond to notices and help parents monitor the online activities of their children and filter unwanted content[9].

The eSafety Commissioner can investigate complaints about prohibited or potentially prohibited content. If the content is hosted in Australia, the eSafety Commissioner can order the take-down of material using powers in Schedule 7 of the Act. If the content is hosted outside of Australia, the eSafety Commissioner can report it to law enforcement and advise links to the makers of internet filters using powers under Schedule 5 of the Act. Schedule 7 extended regulation to live streamed content services, mobile phone services and services that provide links to content.

My review of the online content scheme responds to my terms of reference and, in particular, considers the relevance and effectiveness of the online content scheme and what changes might be made.

Not Fit for Purpose

It is hard to see how a piece of broadcasting legislation developed in a different age, covering markedly different companies, could be equally appropriate to the rapidly evolving digital era.

Traditional television and radio broadcasting services are generally provided by large companies that are licensed and tightly regulated in the public interest, underpinned by a co-regulatory framework in Australia. Online services are quite different—they vary enormously in size and function, operate without geographic borders, are not licensed in the same way as broadcasters and, having effectively won the public argument that they were just pipes used by others to transmit data[10] or not legally liable for the content on their platforms[11], are rarely tightly regulated. And, so it seems with the scope and nature of the online content scheme.

The original set of online content rules in Schedule 5 were introduced at a time when content accessed via the internet meant accessed via a computer connected to a physical data line. With the proliferation of mobile devices, the next set of rules introduced mobile content in Schedule 7. This introduced discrepancies between how the same piece of content could be treated, depending on whether it was accessed via the internet or via a mobile carrier content service. Following the introduction of mobile data services, this technological distinction became irrelevant[12].

[9] Australian Law Reform Commission, Classification—Content Regulation and Convergent Media: ALRC Report 118 (2012).

[10] This is the carriage service argument put by traditional internet service providers.

[11] Organisations like Facebook argue that they are not publishers and play no editorial role in respect of user generated content and are therefore not legally liable for the content posted on their platforms—an argument based on the safe harbour provisions of the US *Communications Decency Act*, which the online industry argues is essential for free speech.

[12] Optus submission, page 6.

In this review, I found consensus that linkage to content type and technology in the online content scheme was out of date and no longer fit for purpose, having failed to keep up with consumer preferences and technological developments over the last 15 years, and not being reviewed and updated regularly to ensure consistency and relevance. This is most effectively illustrated by the absence of smart phone legislative coverage in a country dominated by smart phones, and is replicated by the failure to cover other content delivery models, such as short range wireless communications technology like Bluetooth, cloud computing and apps. To maintain currency, the legislation needs to be, as far as is possible, technology neutral.

I found that neither Schedule is distinct. Both contain near identical provisions. Duplication across the Schedules undermines their clarity, making them difficult to interpret and hard to understand, and presenting a significant compliance challenge for both industry and the regulator.

Telstra[13], for example, has obligations as an internet service provider, a hosting service provider and content service provider, which create different pathways and involve multiple provisions that create technical compliance challenges and a fragmented approach to dealing with online safety issues. Moreover, Optus argues that:

> *"[t]he current level of prescription in the existing schedules, especially the attempt to capture and specify rules for every single type of online content provider is unhelpful and leads to confusion and high levels of complexity for providers. It requires significant investment in resources in managing compliance, difficulties in enforcement by the regulator, and reduced consumer protections."*[14]

The online content scheme is a piecemeal regulatory scheme that lacks coherence and consistency with other offline media and broadcasting frameworks.[15] This results in inconsistent treatment of the same content across different platforms.

Arguably, the same piece of content should always be treated the same, regardless of how it is delivered to audiences. Further, the legislation would be more powerful if its treatment of different technologies and devices could be as generic and all-encompassing as possible, rather than running to detail.

The regulatory system should target what the online industry does, rather than who or what they are at any particular time in their lifecycle.

Finally, the way the Schedules are written creates challenges for everyday Australians to understand how the provisions operate and what is actually covered.

[13] Telstra Corporation Limited submission, page5.

[14] Optus submission, page 8.

[15] For example, the approach to MA15+ content under Schedule 7 is inconsistent with other platforms, such as the commercial television code of practice which allows for free-to-air broadcast of MA15+ rated material within prescribed times. Similarly, the approach to X18+ content, which is content prohibited online, is inconsistent with provision offline in the ACT and NT where the sale of X18+ material is legal.

The Australian Law Reform Commission argued in their *Classification—Content Regulation and Convergent Media: ALRC Report 118 (2012)* that the requirement for industry to prohibit X18+ online content hosted in Australia is "*largely symbolic, given inconsistency with classification arrangements for offline media and the proliferation of overseas providers hosting X18 material*". It recommended that all adult content (R18+ and X18+) be restricted to adults. This would make it legal for Australian-based service providers to provide X18+ content, albeit behind a restricted access system.

The Australian Law Reform Commission found general consensus in its review work undertaken in 2012 that the *Broadcasting Services Act* provisions regulating online content were *"highly complex and confusing legislation that is almost incomprehensible… and legally uncertain"*.[16] The information presented to me supports that summation.

I find that the online content scheme is not fit for purpose and recommend that it be replaced.

Effectiveness

The effectiveness of the online content scheme would ideally be measured against the framework in which it operates and the level of consumer protections provided in response to threats to online safety. It has been challenging to get a clear picture of either due to the highly competitive, inventive and dynamic nature of the online industry and the absence of reliable data on which to draw conclusions. But there are some operational factors that shed some light on the effectiveness of the scheme.

Industry and Regulator Activity

Australia's first line of defence against prohibited online content is the online and digital industry, which generally relies on algorithms, their own technology, advanced commercial solutions and filtering mechanisms to identify and take down illegal content. Australian based companies also block the INTERPOL "worst of" list of child sexual abuse material hosted on websites.

I understand that global companies like Facebook and Google take down millions of pieces of inappropriate content each year, which is vastly more than the 10,000–13,000 or so items the eSafety Commissioner deals with each year as part of the complaints-based system she administers.

Nevertheless, the eSafety Commissioner and the ACMA and ABA before it, have had considerable success as a safety net in getting illegal content taken down by Australian industry hosts within 24 hours. I am pleased to report that there has been total compliance with all Australian take-down notices issued since the online content scheme was introduced[17].

I found that the regulatory regime has been highly effective in Australia—there has been a reduction in illegal material hosted in Australia, reflecting the success of industry actions and regulator take-down compliance.

We are now experiencing an apparent growth in overseas hosted material. Indicative of the trend to overseas hosting is the fact that the eSafety Office took down no online content hosted in Australia in 2016–17 and 2017–18, but assisted in the facilitation of the take-down of more than 5000 child sexual abuse items hosted overseas in 2016–17 and more than 8,000 such items in 2017–18. According to submitters to this review, it now appears that, with the passage of time, the eSafety Office's initial focus on take-down notices in Australia is becoming less efficacious and valuable due to the migration of illegal content from domestic websites to websites hosted offshore[18].

This does not in any way suggest that a strong continuing Australian focus is not necessary; it merely illustrates that those intent on illegal activity are inventive and agile in their efforts to get around the law and associated regulations and will move around the world electronically to do so.

[16] Australian Law Reform Commission, *Classification—Content Regulation and Convergent Media: ALRC Report 118 (2012)*, page 58.

[17] *Office of the Children's eSafety Commissioner Annual Report 2015–16*, page 126. No take-down notices were issued in 2016–17 or 2017–18.

[18] Communications Alliance and Australian Mobile Telecommunications Association (AMTA) submission, page 5.

Some submissions to this review emphasise the escalating nature of community concern about harm online; opportunities for user access to dangerous content; and the potential for serious downstream consequences. These concerns raise issues about the online industry's social license to operate.

One submission argues, for example, that the challenge to regulators in the online world is vastly different to the historical challenge faced by customs services of detecting and seizing books, films and videos at the border; with "*illegal and abusive materials now e-travelling relatively unhindered across borders, leading to copycat behaviour and contributing to sexual assault*"[19]. Collective Shout takes this one step further by arguing that the current system is limited because it fundamentally "*fails to adequately address the global nature of the cyber world and the real harm to children and women caused by the pervasive nature and global flood of pornography … [in a] culture where prohibited things like the rape and murder of women are permitted, eroticized and the object of laughter*".[20]

Whether there is a direct causal link between online pornography and violence is contested[21], which highlights the difficulty in reconciling the tension between the view that adults should have the right to access non-violent pornography online, and the generally accepted view that children should be protected in some way from being exposed to pornography online.

Local Australian take-down actions have needed to be matched with increasing engagement with INTERPOL through Australian police services and the European based INHOPE[22] because almost all of the harmful material now appears to be hosted overseas, where the eSafety Commissioner has no direct powers. That engagement has resulted in rapid take-down of the vast majority of material in its host jurisdiction (generally within 3 days) after the eSafety Commissioner has approached INHOPE to facilitate the take-down via its extensive international network. The eSafety Commissioner reports that the INHOPE take-down system has been highly effective in taking down illegal material and harmful images—with 85% of the 85,000 child sexual abuse material cases hosted in the clear web reported to it in 2017 being taken down.

Disturbingly, as some illegal sites are closed down, new ones are opening up. A number of members of the INHOPE network are now contending with extensive volumes of child exploitation material provided via clear-web file hosts. According to the eSafety Commissioner, there is an opportunity for disruption of the business model of these evil file hosts in Australia by denying them the use of top-level domains, hosting networks, advertising networks and payment facilities. Such an approach could be covered by standards in the new legislation or by the proposed mandatory industry code of practice. Clearly, there are also opportunities to engage and collaborate with law enforcement around business disruption approaches.

[19] Confidential submission.

[20] Collective Shout submission, page 6.

[21] See discussion in the United Kingdom House of Commons Women and Equalities Committee, *Sexual Harassment of women and girls in public places: Sixth Report of Session 2017–19*, October 2018, https://publications.parliament.uk/pa/cm201719/cmselect/cmwomeq/701/70102.htm.

[22] The Miscellaneous sections of both schedules enable the eSafety Commissioner to liaise with regulatory and other relevant overseas bodies about co-operative arrangements for the regulation of the internet industry, including arrangements to develop multilateral codes of practice and internet content labelling technologies.

Codes of Practice and Industry Standards

Codes of practice have historically been a very important way for industry to develop effective co-regulatory arrangements in the Australian broadcasting and telecommunications sectors. There are currently four voluntary industry codes for the online content scheme[23], but the main codes operational in the online industry are the internet industry codes of practice for internet and mobile services which seek to ensure that restricted and prohibited content is not available to end-users. I am satisfied that the codes in the Schedules have harnessed industry attention on illegal and harmful content and have served to reduce the amount of such harmful content that would otherwise be available and, in their present form, provide a reasonably effective shield against inappropriate material.

However, I heard in this review that the overly prescriptive nature of Schedules 5 and 7 has prevented a meaningful overhaul by industry of the industry codes—because the codes cannot be changed unless associated parts of these Schedules, are changed first. As a result, the industry codes are either out of date or redundant, and reliant on changes to legislation to enable code review and rewriting. Moreover, Schedules 5 and 7 do not enable the eSafety Commissioner to unilaterally order a new code. Even if this was possible, any new code would simply import the deficiencies of the current legislation, rendering the industry still unable to comply owing to the prescriptive elements set out in each Schedule.

This means that the current take-down and filtering system is more reliant on individual company policies and the goodwill of industry players, than might usually be expected with an industry code, which suggests a fault in the co-regulatory framework.

In the wake of these problems and although the eSafety Commissioner maintains relatively strong relations with key private operators in the online space, a number of submitters to this review have suggested that the eSafety Commissioner should do more to compel industry to deliver on their co-regulatory responsibilities—by promoting the strengthening of industry-based interventions that would help to improve collaboration between industry and government against dangerous or illegal material.

The eSafety Commissioner is empowered by the online content scheme to make an industry standard in limited circumstances. She may make a standard if a direction to make an industry code is not complied with or where there is no relevant industry body appropriate to make a code. She may also make a standard where there is a code in place and there is evidence of the partial or complete failure of the code. It is surprising that, in this period where few codes are operating effectively, the eSafety Commissioner has elected not to create any standards. This illustrates the clear tension between a system increasingly reliant on industry relationships and good will and parts of the industry intent on minimizing regulation, against rising community expectations about government intervention to ensure protection from online harm.

As we move forward, it will be important for the eSafety Commissioner to be enabled to independently establish new standards and operating principles for industry. It is clear that the four current codes are out of date, and should be replaced.

[23] The Content Services Code and the Internet Industry Codes of Practice—Internet and Mobile Content (consisting of three codes).

I found that there should be a single new fit for purpose and technology-neutral code of practice. This single code would fulfil a wider purpose than the current codes—it would set the behaviour benchmarks and compliance requirements for industry around all aspects of online safety, covering all Australian end-users. Further, I consider that the legislation should empower the eSafety Commissioner to create an industry standard or standards, irrespective of code arrangements in order to provide her sufficient flexibility to respond quickly to emerging harmful activities[24].

Some contributors to this review have questioned the need for codes of practice at a time when black letter law might be more effective in regulating the system. I found that it will be necessary, nevertheless, to have an industry code in place for many years to come in order to:

- develop the operational and organisational practicalities of the legislation for successful on-the-ground implementation
- ensure that detection and prevention activities are managed as far as is possible by the digital and online industry, and
- create a dynamic environment for continuous improvement in detection methods by industry.

The core of the proposed new single code will need to be technology, device and platform neutral.

It is therefore important that the eSafety Commissioner commence consultative work as soon as possible with the digital and online industry on a new legislative standard governing the new code and new code requirements.

I recognise that the default position of industry is that it wants to be left alone by government[25]. I am also conscious that industry codes can potentially have little effect if an industry player or players chooses not to sign onto a code or comply with it. Recent examples before the Royal Commission on Financial Services show how relatively easy it is for industry to not pay due regard to compliance when they are focused on profit making.

In the circumstances, I recommend that compliance with industry codes be mandatory for all industry participants with online and digital activities in Australia (including overseas participants), in a framework to be administered by the eSafety Commissioner, with appropriate penalties for non-compliance. As these new code arrangements will be a significant new task for the eSafety Office, additional resources will be required.

Other Mechanisms

There are other mechanisms operating to assist Australians manage online content. For example, the Communications Alliance is currently undertaking a program of work to reinvigorate the family friendly filter scheme, and anticipates that new players will enter the field. There are now three companies registered to provide filters under the family filters scheme, which has increased the program's effectiveness from the one registered company operating earlier in 2018.

The availability of filtering technologies provides families with some confidence that they can control at least some parts of their children's internet usage at home. I would expect to see such filtering technologies included in a new industry code as part of a suite of measures comprising the protection from online harm regime, but I do not see the need for the scheme to be prescribed in the legislation. If code coverage is deficient, the eSafety Commissioner should have the power to make standards.

[24] At the moment, such a reserve power to make a standard is provided for under Schedules 5 and 7 but not in the *Enhancing Online Safety Act*.

[25] From the speech by the eSafety Commissioner to the National Press Club, 3 October 2018.

In addition to this, there are other mechanisms the industry uses to provide online safety, which include safe modes, the ability to enable restrictions to allow parents to control purchases or restrict inappropriate content from appearing within search results, the explicit prohibition of sexually explicit, overly violent materials on platforms, and a variety of educational programs.[26] These and other mechanisms are to be encouraged, possibly by inclusion as code requirements.

The Classification System

The online content scheme relies on the National Classification Board to classify online content in order for the eSafety Commissioner to issue a final notice to an Australian content host. As online content falls into the definition of film in the *Classification (Publications, Films and Computer Games) Act 1995* (Classification Act), the Board's classification system, timelines and processes are based in film classification requirements[27]. These arrangements stand in stark contrast to today's web content which is dynamic, highly interactive and immersive, often served up in ways that cater to user preferences, and delivered in significantly greater volumes through user generated content than for any film[28], and in real time to all age groups.

I found in this review that the Board's statutory turnaround time of up to 20 working days for a classification decision makes no sense because it is out of step with the 24/7 immediacy of the online world. Even priority applications, which are to be concluded within 5 working days, fail to recognise that instant take-down of online child abuse material is required.

Further, the online content scheme's requirement to use the Board in these circumstances fails to recognise the eSafety Commissioner's expertise in child abuse by not empowering her to make classification determinations, even though the Schedule provides for trained content assessors outside government to do so. Moreover, less and less internet content is being referred by the eSafety Commissioner to the Board, with 37 referrals for classification in 2015–16, four referrals in 2016–17 and none in 2017–18, as creators of online child abuse content are hosting it overseas.

Reliance on a classification system that is focused, amongst other things, on allowing adults to make informed choices about what they read, hear or view is highly questionable when applied to children's safety. The eSafety Commissioner argues that the use of a harm standard would allow the online content standard to operate separately from classification policies and practices as well as allow for faster assessments of content.

> *"Such an assessment… would [prevent] access to content that is likely to do harm (eg preventing children accessing violent and degrading online pornography), or [prevent] access to content production which is harmful (eg child sexual abuse material)."*[29]

Online content providers do not mind how material is classified, so long as it is done correctly, consistently and quickly, and does not vary between media or technology.

[26] Communications Alliance and AMTA Submission, page 7.

[27] The Board is required to make decisions in line with the *Classification (Publications, Films and Computer Games) Act 1995*, the National Classification Code and the Guidelines for the Classification of Films.

[28] Office of the eSafety Commissioner Submission, page 58.

[29] Office of eSafety Commissioner Submission, page 59.

I recommend that the classification system applying to online content be changed. The most effective online safety classification environment is likely to be one where prohibited and illegal classifications are maintained (to ensure enforcement) and supplemented by a new harm standard, with the eSafety Commissioner and her office empowered to make classifications and to determine harm standards. Harm standards would need to be carefully crafted to provide safeguards against the risk of over-censorship, and potentially to provide different levels of protections for adults and children or utilize access limiting technology, such as restricted access systems. As part of this arrangement, provider assessors would continue and would be retrained in the new arrangements and certified in a joint ACMA/eSafety Commissioner function.

International models

The terms of reference required me to provide an assessment of other regimes, including international models, in dealing with prohibited content that is hosted overseas. It is clear that many countries are struggling with the same issues as Australia, and are trying out many of the same forms of prevention and take-down arrangements for harmful material.

Governments and major players in the industry now accept that some form of regulation is necessary.

From late 2017, Germany's *Netzwerkdurchsetzungsgesetz* (*Network Enforcement Act*) requires internet platforms with more than 2 million users to have reporting systems for hateful posts and to delete reported content if it is illegal under the German Criminal Code. The Act doesn't prohibit Germans from posting illegal content, and puts the onus on platforms to keep only legal content on their sites and delete manifestly unlawful posts within 24 hours, or be fined. If a platform receives more than 100 complaints about unlawful content per year, they must publish a transparency report. Commentary on the *Network Enforcement Act* notes:

> *"[T]he internet cannot go unregulated; while it is free space, the social media platforms that people use on the internet are not. Private companies must abide by the law, especially when they have so much influence over society."* [30]

The European Union has adopted a raft of measures (strategies, directives and so forth) to encourage proactive industry engagement with online safety, with varying levels of success. In late 2017 the European Parliament called for more evidence that the measures were working because the industry had failed to provide statistics on the take-down and blocking of websites containing or disseminating child abuse images, the types of blocking used, the speed of content removal, the frequency with which reports are followed up by law enforcement authorities and used to prevent crime, and the security methods used to ensure that blocking lists aren't leaked.

There are lessons for Australia in this, as I have seen very little evidence about the effectiveness of the current Australian regime beyond complaints-based data generated by the eSafety Commissioner. Unlike Europe, Australia does not even attempt to collect data systematically from the industry on the take-down and blocking of websites containing or disseminating child abuse images, the types of blocking used, the speed of content removal, and the frequency with which reports are followed up by law enforcement authorities to prevent crime.

[30] Mikayla Appell, A New Responsibility for Internet Platforms: Germany's New Hate Speech Law (23 January 2018), American Institute for German Studies, www.aicgs.org/2018/01/a-new-responsibility-for-internet-platforms-germanys-new-hate-speech-law/.

I recommend that the eSafety Commissioner be empowered and resourced to do so through the legislation, and that she should publish this information alongside her own compliance data in an annual report. This would mirror reporting arrangements in the energy market and in telecommunications, and would most certainly increase the understanding of what is happening in the online safety world. It would also provide an evidence base for policy decisions and identifying systemic compliance issues.

In June 2018, the European Parliament adopted an extended Audiovisual Media Services Directive to ensure that children are protected from harmful content (through tools to report and flag harmful content, age verification and parental control systems); to make the most harmful material very difficult to access; and by encouraging industry in all European countries to develop common content descriptors to help parents regulate their children's use of the digital environment. These rules are to be enforced by national broadcasting regulators.

The European Commission has just announced that it will regulate to require hosting service providers (such as social media, video and image sharing platforms, cloud services and online newspapers) to remove terrorist[31] content within one hour of receiving an order from authorities, and require service providers at risk of exposure to terrorist content to adopt proactive measures, such as automated detection tools, to reduce the accessibility of terrorist content online.

In November 2017, a private member's bill was introduced into the Irish Parliament proposing a system that appears to be modelled closely on Australia's eSafety Commissioner's functions[32]. If the bill is enacted, Ireland will establish a Digital Safety Commissioner to regulate and oversee a take-down procedure, to be operated by digital service providers free of charge. The Digital Safety Commissioner will develop a code of practice for the take-down procedure and develop national online safety standards with which digital service providers must comply. The Commissioner will be able to apply to the Circuit Court for enforcement of a direction. In addition, they will provide education, research and information sharing and co-ordination of government activities. Facebook Ireland has criticized the proposal on the basis that, in the absence of a definition of harmful communication, the legislation risks uncertainty, unpredictability, and limiting freedom of expression.

In July 2018, the Irish Government released an Action Plan for Online Safety that acknowledged the Commissioner model, but noted that its progression may be slow for reasons of jurisdictional and legal complexity, and that specific actions proposed in the plan were not dependent on its passage. The actions proposed in the plan include: a national advisory council to government; legislation to provide for criminal offences; a national communication campaign and single identity and online access point for online safety; and a cross-government co-ordination body to ensure a coherent and united policy approach.[33]

New Zealand's *Harmful Digital Communications Act 2015* makes it an offense to harm by posting digital communication, with those so harmed applying to the District Court for fines and a range of orders to remove material; cease conduct; and publish a correction, an apology or a right of reply. Online content hosts have a safe harbour from liability, so long as they have a complaints mechanism, which is open to users and Netsafe (an independent, not for profit approved agency under the legislation).

[31] Terrorist content means material and information that incites or advocates the commission of terrorist offences, encourages the contribution to terrorist offences, promotes the activities of a terrorist group, and instructs on methods or techniques for the purpose of committing a terrorist offence.

[32] Digital Safety Commissioner Bill 2017, http://www.oireachtas.ie/en/bills/bill/2017/144/. At the date of writing, the bill had not progressed through the Irish Parliament.

[33] The Office for Internet Safety, Department of Justice and Equality, *Action Plan for Online Safety 2018–2019*, www.internetsafety.ie/en/IS/Pages/PB18000003

New Zealand's Act is broader than Australia's legislation because it covers harm to both children and adults, and its definition of online content hosts includes communications sent by email, mobile phones and posted on websites and social media sites. However, unlike the eSafety Commissioner, Netsafe has no take-down powers and must apply to the District Court, which is a serious deficiency in the model.

This strongly legislatively based model is not relished by the industry, with Microsoft[34] arguing that the civil and criminal enforcement processes were "*novel, untested, and not necessarily the most efficient way to achieve the Government's objectives of mitigating harm and providing victims with a quick and efficient means of redress*".

The United Kingdom came to the area late, but now has one of the most active approaches to children's online safety in the world and has, arguably, surpassed Australian efforts in recent years, through:

- A Digital Charter, which is a rolling program of work to agree norms and rules for the online world and put them into practice so that the UK will be the safest place in the world to be online.
- The *Digital Economy Act 2017*, which requires age 18 verification for access to commercial pornographic websites and applications if they are to avoid the risk of being shut down. For sites operating outside the UK, the Act forces local businesses (such as online payment services or those buying advertisement space) not to deal with offending sites in order to close off their revenue sources.
- The UK Government's response in May 2018 to the Internet Safety Green Paper, which includes: a social media code of practice and transparency reporting; that companies need to take a more proactive approach, which preempts issues on their platforms before they occur; further development of technical solutions to tackle online harms as well as an emphasis on online safety materials and education; consideration of the legal liability that social media companies have for content shared on their sites; and release of a White Paper later this year.

The British legislation has widespread community support, including from the local pornography industry and the Canadian internet pornography giant, MindGeek. Opponents cite circumvention and enforcement difficulties for non-UK companies, privacy, freedom of speech, unnecessary government intervention, and failure to address social media sources of sexual content for young people as reasons for their stance.

It is clear that many overseas governments are cranking up their regulatory oversight of the online space. There is much that Australia can learn from the European and British experience and practice, in particular their proposals for a rolling program of containment work; greater reliance on industry to take preemptive action; using third party businesses to block offending sites in order to remove their revenue source; and data collection. The other important implication is that no regulatory system can remain entirely effective in addressing prohibited content (unless the internet is fully centrally controlled), so free-world countries must keep taking action to deal progressively with new abuse and misuse mechanisms as they arise.

[34] Summary of submissions made to New Zealand Justice and Electoral Commission in 2013.

Statutory Review of the *Enhancing Online Safety Act 2015*

The *Enhancing Online Safety for Children Act* was introduced in 2015 and renamed the *Enhancing Online Safety Act* in 2017 when its coverage was extended to certain adults (including older Australians at risk of online harm and people at risk of family or domestic violence) experiencing image-based abuse. That change broadened the role of the eSafety Commissioner to enable her to address online safety for all Australians and to conduct promotional activities, research and provide advice. Importantly, the Act provides for the eSafety Commissioner to take an online safety leadership role for all Australians.

The eSafety Commissioner has regulatory responsibility for online safety and works with internet and content service providers to have harmful material taken down quickly. More specifically, the Act sets up the administrative arrangements for the eSafety Office and enables the eSafety Commissioner to administer:

- the cyber-bullying complaints scheme, which investigates serious cyber-bullying of children
- the online content scheme (under Schedules 5 and 7 of the *Broadcasting Services Act*), which investigates offensive and illegal online content, prioritizing child sexual abuse material, but also covering content advocating terrorism, incitement to crime or violence, and sexually explicit content, and
- the image-based abuse scheme, which provides a reporting and investigation mechanism for the non-consensual sharing of intimate images
- in addition, the eSafety Commissioner's role includes research, prevention, awareness raising and education.

The *Enhancing Online Safety Act* provides a complaints regime for cyber-bullying of children on social media or a relevant electronic service. The eSafety Commissioner oversees a two-tier system for rapid removal[35] by industry of cyber-bullying material from social media services—with tier one social media services being requested to remove bullying material voluntarily and tier two services being given a notice requiring the removal. Tier two services are the largest social media companies (namely Facebook, Google+, Instagram and YouTube).

The eSafety Commissioner may also give an end-user notice to a person who posts cyber-bullying material against a child, requiring them to remove the material, refrain from posting more material, and apologise to the child. To date, the Commissioner has not issued any end-user notices.

The legislation enables the eSafety Commissioner to disclose information to schools, parents, and certain authorities if she is satisfied that the information will help resolve the complaint or assist other authorities fulfil their functions, and if permitted to do so by the person concerned.

Further, the Parliament has recently passed the *Enhancing Online Safety (Non-consensual Sharing of Intimate Images) Act 2018*, which from 1 September 2018 extends the eSafety Commissioner's functions under the *Enhancing Online Safety Act* to a civil prohibition and penalty regime applying to social media, relevant electronic and internet services and end-user perpetrators, with associated take-down powers for the non-consensual sharing of intimate images.[36] The amending legislation also created new criminal offences for using a carriage service to distribute private sexual material that carry

[35] Within 48 hours.

[36] Which refers to the sharing or distribution of an image or video of a person(s) portrayed in a sexual or intimate manner, which has been shared without their consent by a social media service, relevant electronic service or a designated internet service.

penalties of imprisonment for up to seven years[37]. The eSafety Office advises that it has started to receive complaints, conduct investigations and use its civil formal and informal warning powers.

Effectiveness

The current eSafety Commissioner has built upon the success that the eSafety Office has achieved since it was established in 2015. In the words of the Department of Home Affairs:[38]

> *"The eSafety Office fills a genuine need for effective action where a criminal justice approach may not be appropriate or preferred by the affected persons. In particular, the eSafety Office's online safety education measures and resources, civil resolution and enforcement options, and remit to take-down prohibited online content and image-based abuse are valuable tools."*

I found considerable evidence throughout these reviews that the eSafety Commissioner is doing a very good job, especially in terms of her work with industry to bring about online safety improvements, her promotion of online safety issues, and the delivery of rapid and responsive online protections to Australians. Her energy, drive and passionate pursuit of an internet and digital environment that is open, free and safe has delivered a sea change in policies and online safety activity.

I also found in these reviews that there is widespread support for the eSafety Commissioner's work and that of her Office, even though their work has been somewhat constrained by the limitations on her powers, out-of-date legislation, and governance arrangements.

Adequacy of Coverage of Cyber-bullying Complaints Scheme

It is important to understand that the cyber-bullying complaints scheme isn't the only answer to online safety. The scheme is a complaints-based safety net regime that takes effect only after other preventative and take-down options have been exhausted—namely if industry detection, blocking and filtering fails. The scheme requires people experiencing online harm to approach the content provider first to take the offending material down and, if that fails, they may then approach the eSafety Commissioner who may intervene with industry to get it to take down the material within 48 hours.

On top of that, the scheme has many of the same limitations as are apparent for the online content scheme—coverage of new or different platforms, mechanisms and devices, and inconsistent and overlapping arrangements.

Many submissions to this review expressed genuine concern that, in order to ensure its continued effectiveness, the cyber-bullying scheme must be able to cover abuse and bullying material across the full spectrum of digital devices, services and platforms that enable cyber abuse to occur due to their interactivity capabilities. When a young person is targeted and cyber-bullied, for example, it isn't just on one platform, it tends to be on multiple platforms so the siloed thresholds of the industry's preventive arrangements tend to miss the total context.

[37] Amendments to sections 473.1 and 473.4 and insertion of new section 474.17 into the Criminal Code. The review of online safety-related criminal offences was outside the scope of my terms of reference.

[38] Department of Home Affairs submission, page 3.

According to the eSafety Commissioner's submission, there is uncertainty as to whether certain online service providers that permit the distribution of cyber-bullying material (such as anonymous apps and various gaming services) are able to be considered as being within the current definition of a social media service in the legislation. Further, the advent of augmented reality, virtual reality, live streaming, 5G, massive multiplayer online gaming and the internet of things/connected devices has resulted in a multitude of different platforms that enable more Australians to be targeted for online abuse. If those platforms and technologies are not regarded as a social media service, there is a risk that they will not be covered by the current legislation as the eSafety Commissioner's powers to require removal of cyber-bullying material are limited to social media services. This uncertainty as to who and what is in or out of the regulatory regime makes investigation, compliance and enforcement unworkable.

Added to this, the prevalence of encryption networks and the dark web are making it more challenging to detect and disrupt child abuse material. There is an additional consideration mentioned by the eSafety Commissioner as to whether app stores should be given more responsibility under the online safety scheme because they could potentially serve as valuable choke points to prevent the spread of illegal or harmful material.

I recommend that the legislation be redrafted in such a way as to embrace all relevant platforms, services, distribution mechanisms and devices and the future state of online and digital communication in a way that is technology and platform-neutral as far as is possible, recognizing that the online industry is unlikely to ever be in a steady state.

I acknowledge that it won't be easy to do this because new technologies and online mechanisms are being invented all the time. But, the success of the approach will remain limited if the legislation continues to contain lists of platforms, services, distribution mechanisms and devices that need to be updated regularly.

A much better approach is for Government to adopt the principle that any device, technology, platform, service or distribution mechanism operating in the digital and online world in Australia is covered by default, whilst allowing the eSafety Commissioner the discretion to ensure coverage of new technologies and mechanisms as they are invented and to exclude others rolled in inappropriately so that business is not impeded unnecessarily. This could be done in standards or instruments made by the eSafety Commissioner.

The comprehensiveness of such an approach would have the added benefit of enabling the rigidly program-based emphasis of the work of the eSafety Office to be removed, thus enabling funds, resources and staff to flow freely to the areas of online safety most in priority need of the Office's attention at any particular time. A number of submissions to these reviews argued that cyber-bullying of children, for example, is given too great a priority relative to other responsibilities. Redrawing program boundaries under a single online safety outcome and establishing a single comprehensive prevention and detection program and regulatory arrangements would help target effectiveness.

I am aware that the eSafety Office administers some programs with specific funding attached, such as the Digital Literacy for Older Australians program—these targeted administered funding arrangements would continue.

The Rapid Removal Scheme

I found in this review that the success of the cyber-bullying scheme is increasingly based on the speed of take-down, which is regarded by affected children and parents as the most important element of any response. I am pleased to say that the speed of take-down in the cyber-bullying scheme is usually less than the legislated requirement, which makes the regime highly effective for Australians. A new standard of 24 hours for take-down for Australian hosted material could be imposed without imposing any stress on the administrative system.

Despite its success, the participation of social media companies in the two tier system for rapid removal of cyber-bullying material requires mention as an indicator of the lengths the major social media companies will go to to avoid being seen as voluntarily co-operating with regulators. Companies with the reputations, influence and resources of Facebook, Google+, Instagram and YouTube should be ashamed that they did not sign up for the tier one voluntary compliance regime. This leaves the strong impression that these companies could easily be doing much more to remove harmful material voluntarily at source; and I consider that they have a social and moral obligation to do so.

I recommend that the two-tier system for cyber-bullying on social media services be discontinued and replaced with an arrangement whereby new legislation would set out the online safety requirements that industry is to meet more generally, with the eSafety Commissioner regulating the system for compliance.

Reactive or Proactive

Throughout my review work, I have heard of the good work being done in many parts of the industry, but I have also been struck by the reactive nature of current online safety arrangements, with reliance on the person being bullied or experiencing harm to know how to complain and who to complain to. Going first to a service provider about such a personally distressing experience as online abuse or cyber-bullying cannot be easy, and necessarily involves some delay before take-down either by the provider or on direction from the eSafety Commissioner, if it is not taken down voluntarily by the provider. In the meantime, significant harm may be being done to the complainant, particularly if the material is on-forwarded as is so commonly the case.

I am advised, for example, that much of the image-based abuse being reported to the eSafety Commissioner is very disturbing and risks putting affected people in harm’s way. I recognise that it is not always easy to detect such material at source, given the nuances of consent and freedom of expression. However, if there is clear non-consensual sharing and if there are means to do so, I can see no justification in waiting until the affected people complain before this material is taken down.

I found in these reviews that most social media companies recognise the need to proactively manage their online services to weed out inappropriate and harmful material at source. Indeed, most if not all social media services have online safety policies that align with promoting online safety on their platforms. Compliance with such policies often forms part of user terms and conditions.

But, it is not enough to just recognise a need or to have a policy. Despite arguments to the contrary by some parts of the industry, I understand that what is taking place much less often is the actioning of those policies. In other words, not all companies in the online industry are proactively patrolling, detecting and removing toxic or illegal content from their platforms, nor are they enforcing their own online safety policies and behavioural standards. There is a pressing need for a more proactive online safety regime to ensure that this occurs.

Current legislation only requires technology companies to comply with minimum safety standards, but there is much more that they could be doing to proactively detect and stop harmful content at its source through the application of technology and human intervention. The practice to date has largely been one of retrofitting child protection safeguards into online services and products after harm emerges, or the damage is done. It would be much more effective to protect users upfront.

I recommend that the online safety regime be more proactive in taking down harmful content and in preventing its upload. The proposed new legislation should require industry to implement proactive protective measures. Their activities should be reported annually to the eSafety Commissioner, with severe penalties applied for non-compliance.

A more interventionist enforcement regime will require the eSafety Commissioner to engage experienced investigators with a strong commitment to transparent and robust compliance. This will require additional resources, and will necessarily involve a level of cultural and practice change within the eSafety Office as it becomes a more active regulator. At the same time, as I will discuss later, the eSafety Office and law enforcement will need to work more closely together to detect and deter the posting of illegal material.

As part of a stronger preventive strategy, I consider that the eSafety Commissioner should be given the power to embed more protection for online users at the design stage of new online products. Safety by design could have a significant preventative impact in the digital world where new products are being developed all the time. The safety by design process might involve the following principles:

- platform responsibility—so that the burden of safety does not fall solely on the end-user
- recognition and respect for user identity—reflected in age-appropriate design of services
- user empowerment—so that users can control their own personal safety and privacy, and
- transparency and accountability.

Among other things, the eSafety Commissioner could also provide safety by design advice to industry about:

- implementing PhotoDNA, indexing tools such as web crawlers, and text analysis algorithms to detect grooming, harassment or incitement to crime
- drafting effective terms of service prohibiting illegal or abusive conduct, including behavioural thresholds
- creating seamless, co-ordinated and consistent referral routes to law enforcement, and standardised processes to support, protect and advise those impacted by abusive and harmful behaviours online
- ensuring that default-on settings are applied to accounts to ensure privacy, age-based and appropriate protections, location tracking, data collection and account security are at their highest level
- distributing examples of innovative safety practice, links to innovative start-up incubators, and new and emerging online safety technology.

I recommend that safety by design be incorporated in legislation, and provide the basis for a new online safety standard for industry.

Enforcement

The eSafety Office invests a lot of time in supportive work, designed to deal with bullying behaviour at source, once harmful cyber-bullying material is removed. This often involves the school, as well as the parties involved, and I have found the Office's work to be a force for good that should be continued as it seeks to correct inappropriate bullying behaviour and prevent future incidents.

The response adopted by the eSafety Commissioner recognises that young people involved in cyber-bullying or posting self-generated sexual images are still developing in their maturity and do not generally appreciate the impact on themselves or on others of what they are doing. The eSafety Commissioner argues that to penalise them by issuing an end-user notice or reporting them to the police may not be proportionate to the behaviour involved nor appreciate the innocence and the development stages of the young people involved. To back this up, the Commissioner cites youth justice principles, which call for the least restrictive form of sanction, coupled with efforts to educate young people about the potential consequences of their actions, with emphasis being given to the interests of the young offender as well as those of the victim.

The eSafety Commissioner advises that she has not issued an end-user notice because the circumstances warranting such a serious intervention have not arisen. The eSafety Office has been able to work closely with schools and parents which has resulted in defusing the behaviour, so the Commissioner argues that there have not been instances to date where it has merited taking further action.

The Australian Federal Police[39] agree that in the vast majority of these cases, law enforcement isn't the most appropriate course of action. I understand that the usual practice is that the police will not take action without a complaint from a victim in the form of a statement. Even then, they must show that there is a reasonable prospect of conviction, assuming that there are no other less-restrictive means of sanction available under restorative justice or diversionary instruments.

I consider that concerns about being cognisant about teenagers' maturity, growth stages and other vulnerabilities should not be allowed to outweigh the need to report the most dangerous cyber-bullying activity to police. There is a risk that some cyber-bullies could continue a pattern of bullying behaviour into adulthood if they can get away with it when younger; possibly reinforcing the acceptability of threatening, or violent and dangerous behaviours that could endanger the community and their families later on. Interestingly, DIGI argues that end-user notices should play a critical role in deterring abusive online behaviour and changing the way people treat each other[40].

The eSafety Commissioner needs to be balanced and proportionate in how she uses her powers, taking into account the interests of children, particularly in the case of child on child matters. But, this should not preclude her from issuing end-user notices for the worst young offenders and, where the behaviour has reached the threshold of criminality, they should be reported to the police in the various States and Territories involved, and the police should take appropriate action.

I have not been able to determine in this review whether the harmful material reported to industry and the eSafety Office is taken down forever, if it is redistributed later by the perpetrators or others, or that the parties involved do not continue cyber-bullying in one way or another—either against each other or to third parties, or through another digital platform. It is clear that more research is needed in this area and that the eSafety Commissioner should retain and publish data about its referrals and any subsequent police action.

[39] Department of Home Affairs submission, page 5.

[40] DIGI submission, page 4.

No data has been published on cyber-bullying, cyber abuse, and online content cases referred by the eSafety Commissioner to the police. I was advised by the eSafety Commissioner that she has made 10 formal referrals to state and territory police forces about sufficiently serious prohibited online content and 576 formal referrals about sufficiently serious prohibited online content to the AFP in the last three years. As a further indication of the size of this effort, the eSafety Office reported in its submission to the Parliamentary Inquiry into the *Adequacy of existing offences in the Commonwealth Criminal Code and of state and territory criminal laws to capture cyberbullying*, that around 10% of matters are referred to the police but, to the best of its knowledge, none has resulted in criminal charges being laid against children or young people[41].

The civil penalty regime covers the non-consensual sharing of intimate images of all Australians. The eSafety Office's enforcement policy and standard operating procedures give careful consideration to situations where a child is either experiencing image-based abuse or responsible for it. Since the civil penalty regime for image-based abuse commenced on 1 September 2018, the eSafety Commissioner has referred 4 image-based abuse matters to the AFP's Child Protection Assessment Centre. It has also issued 1 formal warning and 3 informal warnings to those posting or threatening to post an intimate image—these warnings are intended to be educative and allow corrective action to be taken, but non-compliance can attract future enforcement action.

The eSafety Commissioner assured me that her Office is keen to work closely with law enforcement when matters have reached a criminal threshold, and has memorandums of understanding with all state and territory police services that guide those referrals. I therefore found it informative that the Department of Home Affairs proposed in its submission to these reviews[42] that the

> *"AFP would benefit from gaining a better understanding of the eSafety Office's policy and processes to assess and determine the matters that require referral to law enforcement, what material and conduct the eSafety Office considers of a 'sufficiently serious nature', and how the eSafety Office determines which law enforcement agency a matter will be referred to. This is of significant importance in relation to information regarding child sexual abuse….The way the eSafety Office interprets this threshold and its general work practices for referrals should be determined more clearly through arrangements between the eSafety Office and law enforcement."*

I found in the reviews that, despite the many very positive working relationships between the eSafety Office, the AFP and other police services, more clarity is needed if enforcement arrangements are to work effectively.

I accept that there is a risk that police enforcement action in this area may not eventuate or may fail due to a lack of priority or insufficient resources, and that community expectations may be raised to a level that cannot be satisfied if police receive lots of complaints on a regular basis about low level online safety issues. However, I am reminded of the Royal Commission findings on the failure of the police system to address institutional child sexual abuse, and I consider it to be most important that this is not repeated for online abuse and cyber-bullying.

[41] Office of the eSafety Commissioner submission to the Senate Legal and Constitutional Affairs Committee, page 3, www.aph.gov.au/Parliamentary_Business/Committees/Senate/Legal_and_Constitutional_Affairs/Cyberbullying/Submissions.

[42] Department of Home Affairs submission, pages 5-6.

I am also conscious that even though there are memorandums of understanding between the eSafety Office and all state and territory police services, the Department of Home Affairs' submission to these reviews suggests that there is sufficient uncertainty around these arrangements that the various criminal thresholds for referrals to the police and the type of matters referred needs agreement nationally between the Commonwealth and the States. The referral situation for the online content scheme is further complicated by the fact that the assessments of content made by the eSafety Commissioner are required to be made against the National Classification Scheme, not criminal legislation—so that different elements are relevant to an assessment for child sexual abuse material by the eSafety Commissioner compared with an assessment of the same content by police.

I am given to understand that some processes between the AFP and the eSafety Office are less than ideal. It is possible that there may be enforcement opportunities that are being missed if the two are not proactively working together to share information, identify and chase perpetrators, and fill gaps in that might maximise the effectiveness of the enforcement regime, such as how to action take-down of terrorist material hosted overseas where there are no established channels of international co-operation.

On top of this, I understand that legal enforcement measures have not been particularly directed at the online industry, even though they can be imposed, but at mechanisms to block or take down inappropriate content. If the rule of law is to prevail online, industry compliance is an area that will need to be ramped up, especially if my recommendations for stronger legislation and standards are accepted.

Co-operative and collaborative relations need to be established between the eSafety Commissioner, the AFP, state and territory police and the Cybercrime Online Reporting Network as soon as possible. The Department of Home Affairs argues that early efforts to second officials between the agencies could be actioned quickly to fix liaison arrangements and manage the interface so that online detection and enforcement arrangements are more in line with community expectations and as effective as possible.

Ultimately, questions regarding liaison efforts between the eSafety Commissioner and police forces may be answered as the design of the Australian Centre to Counter Child Exploitation progresses. Part of the design process should involve consideration of how the eSafety Commissioner is placed to lead online safety education and prevention efforts within the Centre, and how she might assist work to disrupt online platforms distributing child sexual abuse material.

The eSafety Commissioner's Remit

The terms of reference required me to review the eSafety Commissioner's remit, including roles and responsibilities, and whether the current functions and powers in the Act are sufficient to allow the Commissioner to perform her job effectively.

The Office of the eSafety Commissioner was established in 2015 with a remit to co-ordinate and lead children's online safety efforts across government, industry and the not-for-profit community. Consistent with this, Part 2 of the *Enhancing Online Safety Act 2015* sets out the following overarching functions of the eSafety Commissioner:

- promoting online safety for Australians;
- administering a complaints system for cyber-bullying material targeted at an Australian child;
- co-ordinating activities of Commonwealth departments, authorities and agencies relating to online safety for children; and
- administering the online content scheme under the *Broadcasting Services Act 1992*.

The Commissioner has a range of other functions, spread across two Acts, which include research, to make grant payments, monitor compliance, formulate guidelines, and certain disclosure powers. She has specific powers to do all things necessary or convenient to perform these functions. However, I found that the legislation was deficient in not highlighting certain functions (such as incitement to terrorism and her education role) and in its rather fragmented depiction of her roles and responsibilities.

The eSafety Commissioner needs to be front and centre in the fight against online harm, and her role needs to be understood by all. Her role statement needs to be clear and accessible, be principles-based and not be defined by program lists, so that she has maximum flexibility to perform her online safety and regulatory responsibilities.

It is therefore important that all of the functions of the eSafety Commissioner be brought together in a single part of a new Online Safety Act, rather than spread over different Acts and Schedules as they are now, to give greater public clarity to her responsibilities and more enduring practice.

Such clarity would enable the Australian people to develop a proper appreciation of the full range of the work the eSafety Commissioner does and provide a clear go to point for people when they are experiencing online harm. This is especially important because harassment or incitement to wrongdoing generally occurs only occasionally or at certain times in a person’s life, and Australians don’t necessarily know who to turn to. The eSafety Commissioner needs to be widely known as the focal point that all Australians know is available to proactively assist them to manage their online safety concerns where harm is involved.

The key responsibility of the eSafety Commissioner should be online safety and regulation. As part of that responsibility, the Commissioner’s overarching functions should be spelt out in principles, rather than programs, which would include:

- protection of children from online danger and harm;
- safety[43] protection for all people who engage in online and digital communications;
- stewardship, co-ordination and regulation of national online safety harm prevention and avoidance arrangements;
- national leadership in research, education, prevention and behavioural change to reduce harmful online activity;
- industry, community and government engagement for online safety; and
- compliance and enforcement of online safety arrangements.

In addition, to these overarching functions, the eSafety Commissioner’s functions should also include data collection from industry, information dissemination, research, co-ordination of online safety initiatives, best practice recommendations and guidelines, program management, certification or accreditation of programs and providers, and any other activities consistent with her online safety and regulation responsibilities.

There is a fair degree of consensus that the existing powers and functions of the eSafety Commissioner in the legislation are adequate, although not well focused or articulated. As indicated throughout these reviews, a key issue remains as to whether the legislation is sufficiently adaptable and flexible to enable the Commissioner to oversee, for online safety purposes, the full range of digital and other online communications, including new products (such as apps and virtual reality), emerging technologies and presently unanticipated uses for existing products and technologies.

[43] But not including cyber security, which is the responsibility of the Department of Home Affairs and others.

In addition to this, I found that there were four other areas where either the eSafety Commissioner's role is not as clear as it should be or her powers do not currently extend. The first of these is strategy, co-ordination and positioning. The second is that the Act does not specifically flag the Commissioner's important education, prevention and behavioural change leadership role, which I consider to be a serious omission. The third is that the Act is quite limited in its scope to cover adults (excluding them from the cyber-bullying scheme). The fourth is information disclosure and delegation.

Strategy, Co-ordination and Positioning

Throughout the course of this review, I found that submitters supported the eSafety Commissioner's online safety co-ordination role and were impressed by what she and her Office have been able to achieve. Most supported an even stronger role for her in the co-ordination of online safety efforts, which they argued would result in less duplication of services and better leverage of limited resources. Typically, they commented that the eSafety Commissioner should focus on her unique responsibilities (such as leadership, regulation and compliance) and draw more on the expertise of her government, NGO and law enforcement partners in the others (awareness, education and enforcement).

This highlights the need for nuanced and more careful management of relationships by the eSafety Commissioner in order to deal with the highly complex arrangements in which all those working in the online safety field operate. To negotiate this environment effectively, the eSafety Commissioner needs to build stronger relationships with all parts of the sector. She must take steps to enhance co-ordination with the rest of the online safety sector, through respectful and open dialogue with stakeholders, ensuring that the views of others are listened to and that their particular roles are taken into account. It will only be through quality partnerships between the eSafety Commissioner and various players that the huge task of online safety can be more effectively co-ordinated and managed in such a way as to better leverage what everyone has to offer.

At the same time, it is evident that, as her functions have been extended and as new online safety issues have emerged, the eSafety Commissioner has added or been allocated new programs and has developed new responses some of which may have cut across others' responses. There are so many possible online safety responses that it is hard to see clearly what is available much less how they all fit together.

Better co-ordination will necessarily require some change in the way the eSafety Commissioner goes about her work. And, while it might be a hard ask for the eSafety Commissioner, who is used to the freedom to embark on whatever approach she deems necessary to improve online safety, I am confident that adding more discipline to the co-ordination and planning process will result in a partnership that more effectively values others' inputs, embeds change, reduces duplication and better leverages available resources.

A good way to foster stronger relationships and co-ordination improvements would be to reconstitute the Online Safety Consultative Working Group as a standing eSafety Advisory Committee to the eSafety Commissioner[44], with a revised membership and remit. The eSafety Advisory Committee would meet at least quarterly to provide advice on issues and strategy; share research and experience; address issues such as the co-ordination and delivery of education and other harm prevention programs; and begin the process of developing the basis for a rolling program of online safety work.

[44] Although it would need to meet at least annually with both the Departmental Secretary and the Commonwealth Agency Heads Committee on Online Safety.

Co-ordination across the Commonwealth would remain a core function of the eSafety Commissioner. Immediate attention should be given to building the relationship with the Home Affairs portfolio because online safety, cyber security and enforcement arrangements are increasingly intertwined and need to be developed in parallel though collaboration based on flexible and evolving arrangements that harness all opportunities for preventing and managing online harm.

At the Commonwealth level, ideas from the eSafety Commissioner and the eSafety Advisory Committee could be progressed through the new Commonwealth Agency Heads Committee on Online Safety. This will assist the eSafety Commissioner to operate more effectively within central government and provide an excellent sounding board for national online safety initiatives.

Importantly, the eSafety Commissioner's co-ordination and leadership function should also extend nationally to other jurisdictions, industry and the community sector, and to online harms affecting adults. This would establish the eSafety Commissioner as the national focal point for online safety and provide clear impetus to national online safety strategy and co-ordination. This function will entail a mutual commitment to collaboration and relationship management by the eSafety Office and the States and Territories.

More generally, I found in this review that concerns about the eSafety Commissioner's co-ordination role likely point to a much deeper underlying problem with online safety—namely that players in the field have been so busy just trying to manage the challenge of online safety, that they haven't had the time or space to sit back and reflect on what the core components of a national online safety strategy might be and who should do them, much less what an overarching policy might cover.

I therefore recommend that a national online safety strategy in the form of a National Online Safety Plan be developed and effective from 1 January 2020. The new National Online Safety Plan would take its lead from the proposed new online safety legislation, which would set out the core elements of the Government's online safety policy. The National Online Safety Plan would:

- outline the Government's intended regulatory approach to enhance clarity, transparency and accountability
- cover roles and responsibilities within the online sector
- identify major priorities, and
- provide the basis for advising governments on proposed directions.

The National Online Safety Plan would be developed by the Department of Communications and the Arts as the responsible policy agency and the eSafety Commissioner as the responsible regulator and community focal point for online safety, in close consultation with the eSafety Advisory Committee, industry and other agencies across jurisdictions.

The National Online Safety Plan would also inform the development of a national rolling program of online safety work, including implementation and timing arrangements. This rolling work program would be co-ordinated by the eSafety Commissioner and updated regularly on advice from the eSafety Advisory Committee, industry and the Department to ensure its ongoing relevance in the constantly changing online world.

Education and Prevention

The Royal Commission into Institutional Responses to Child Sexual Abuse recommended a greater role for the eSafety Commissioner in online safety education[45]. The eSafety Office is very active in online safety education.

Since 2015, the eSafety Office has rightly given its early attention to taking down abusive material. The last few years saw a continuation of the cybersafety work performed in the ACMA under the Cybersmart banner, after the creation of the eSafety Office in 2015. Since that time, education and outreach around child protection have been informed by the compliance and investigation work of the eSafety Office. The eSafety Commissioner has led their work increasingly into education, not only in response to parental concerns about cyber-bullying of school children and youth suicides, but also because education is an important form of prevention, which should ideally reduce the need for more compliance and enforcement activity down the track.

Now that the eSafety Commissioner has recognised the need to deal with prevention and behaviour change in schools and online, I consider that education, prevention and behavioural change should explicitly be spelt out in legislation as one of the eSafety Commissioner's overarching functions.

I have been convinced by arguments in submissions to this review that, while technological intervention is necessary to address cyber-bullying, it cannot solve what is essentially a social issue which needs to be tackled in schools, in families and in communities. Children can be protected by limiting their exposure to bullying and abuse or by acting to decrease the likelihood of harmful effects. To have an impact, this will require a whole of community approach and a series of preventive measures and harm minimisation strategies, which include parental and carer awareness, education, technology change and regulation.

Sonia Livingston[46] proposes a rethink of the skills children need to engage with the internet so that they do not increase their risk of harm, and suggests that a new skill of social media literacy in children should be developed so that they can manage their online activities wisely and effectively. This makes a lot of sense and is something the eSafety Commissioner should pursue with States and Territories.

I was impressed in this review by the extent to which the education and prevention sector has been very active in the field, but I was equally concerned that education seems to be the most crowded area of community, NGO, industry and government online safety activity.

A number of the players have a very sophisticated approach to dealing with the challenge, and some have articulated concerns that the eSafety Commissioner risks exceeding her scope by cutting across their space or undermining their programs. They argue the need for more collaboration and for the eSafety Commissioner to operate within the norms of competitive neutrality, which would ensure that the non-government sector has room to operate without overlap or duplication.

The eSafety Commissioner maintains that she actively avoids duplicating efforts and resources, and identifies areas of need where the eSafety Office can deliver the most effective results, and that her work is grounded in an evidence base through research and consultation to determine the programs and educational improvements her Office develops. I think the eSafety Commissioner could reflect on overall priorities and on what other stakeholders are doing and what work they might be able to do before committing the eSafety Office to more delivery work that she identifies as new needs.

[45] Royal Commission into Institutional Reponses to Child Sexual Abuse, Final Report (December 2017), Volume 6: Making institutions child safe, page 21 https://www.childabuseroyalcommission.gov.au/final-report

[46] Sonia Livingston, *Developing social media literacy: how children learn to interpret risky opportunities on social network sites*, LSE Research Online, May 2015.

Despite all of this activity, I was surprised to find that there is no agreed national approach as to how online safety and respectful behaviours are addressed in schools. Most States and Territories run schools programs, as do the Catholic and independent schools networks. The eSafety Office produces an enormous array of materials through a number of different programs that might usefully be consolidated and rationalized[47]. The AFP runs the ThinkUKnow cyber safety education program through state and territory police services and various business and community partners[48]. The Department of Social Services also does work with assistance from other agencies on respectful relationships education for young people, which includes the digital environment. Across Australia, governments provide significant funding to the NGO sector for education and support services, often as part of broader mental health initiatives.

Many other providers entered the education field under the voluntary certification scheme. There is concern about the quality of some their programs[49], and the eSafety Commissioner agrees that the scheme should be evaluated and replaced by a much more effective certification arrangement. I found that new certification arrangements are required and that certification should cover both the providers and the quality of their education programs.

Despite this level of activity, eSafety Office research indicates that the most disadvantaged community groups, such as Aboriginal and Torres Strait Islanders and those living in regional and remote areas, miss out. Children younger than school age[50], who are using technology often before they can speak, read or write, miss out almost entirely[51].

All of this points to the desirability of the eSafety Commissioner being given a national leadership role to ensure that there is an overarching online safety education strategy, which recognises and appreciates the roles and responsibilities of the various players in the field and ensures that gaps are mapped, identified and addressed by the appropriate stakeholders.

I found some truth in the argument that the eSafety Office has rushed in to provide new education and training programs and resources whenever the Commissioner perceives a new need has arisen, and that this has created overlaps and duplication and caused disaffection among industry and NGOs at a time when they should all be working together. Then again, I accept that the provision of targeted and free education resource materials against the curriculum has been one of the strengths of the eSafety Office's prevention work, and that these materials are supported by the States and Territories as they have provided a mechanism to enable schools to take immediate steps to inoculate their school and students from online safety risks.

[47] I understand that the major refresh of the eSafety Office's website might assist understanding what is on offer through the Office.

[48] ThinkUKnow has evolved from delivering education to an adult audience of parents, carers and teachers to incorporating school presentations from year 3, and now incorporates age-appropriate cyber messaging and additional law enforcement experiences and case studies. The program helps families understand cyber safety issues and improve their cyber safety security, as well as understand where to report cyber crime, inappropriate behaviour, bullying and child abuse. It has great reach across Australia, particularly into regional areas, and is provided free of charge so is accessible to poorer communities.

[49] The Alannah and Madeline Foundation argues in their submission at page 9 that there are too many sub-standard and unqualified providers; schools have too many providers to choose from; and affluent schools are targeted, while the most vulnerable students miss out.

[50] The eSafety Commissioner, in a 3 October 2018 speech to the National Press Club, indicated that 80% of Australian pre-school age children already use the internet, and 42% of children used internet-enabled devices from age 2.

[51] Except for some coverage on the eSafety Office's iParent portal.

On balance, I consider that the eSafety Commissioner's role in this space should be to provide education leadership, to set quality standards, and ensure that service gaps are filled and met by appropriate service providers. This would include education (including early learning) leadership, social media literacy curriculum co-ordination, pre-service teacher training, and training and accreditation of education providers and programs[52], but not the provision of actual education services to children, which should be left to others providing services on the ground. Only where gaps in service provision cannot be met by others or where the Government deems it necessary for targeted intervention to occur (e.g. in indigenous communities with high levels of child suicide) should the eSafety Office provide education services to children.

Adults

Consistent with prevailing community views over time, Australian Governments have tended to be reluctant to restrict adults' internet use and practice. It is arguable that adults are more than capable of appreciating legal constraints when posting or viewing material, on the one hand, and reporting or coping with online material directed at them, on the other hand.

However, the Turnbull Government recognised the threat of image based abuse against adults as potentially another form of sexual violence when it included revenge pornography as a priority in the Third Action Plan 2016–19 for the National Action Plan to Reduce Violence Against Women and their Children 2010–2022[53] and through amendments to the legislation in 2017, which extended the eSafety Commissioner's remit to certain affected adults. This foreshadowed the introduction of specific legislation about image-based abuse in the *Enhancing Online Safety (Non-consensual sharing of intimate images) Act 2018.*

I found in this review that the tight limitation on the eSafety Commissioner's role with respect to adults flies in the face of the experience of many people (especially women with high profiles, like journalists and politicians, Aboriginal and Torres Strait Islander women, Islamic spokespeople, and the families of murder and rape victims) with online harassment, vitriol, and predator trolling. A number of these women have approached the eSafety Commissioner for assistance.

> *"[In the words of Dunja Mitjatovic] 'Female journalists and bloggers throughout the globe are being inundated with threats of murder, rape, physical violence and graphic imagery via email, commenting sections and across all social media…Male journalists are also targeted with online abuse, however, the severity, in terms of the sheer amount and content of abuse….is much more for female journalists.'…..*
>
> *These dangers do not stay online. Following extreme online harassment campaigns, we have had Women in Media members punched in the street and followed home. A couple of our members have had rape and death threats against them and their daughters."*[54]

Such behaviour is totally unacceptable, and action needs to be taken to prevent it.

[52] But, in a tougher regime than the current certification scheme. It is important that the scheme is evaluated and improved so that it is fully fit for purpose. I understand that the eSafety Office is currently reviewing the certified providers program.

[53] National Priority Action Area 4.6, page 25. www.dss.gov.au/sites/default/files/documents/10_2016/third_action_plan.pdf.

[54] Dunja Mitjatovic quoted on Toxic Twitter and in the Women in Media submission, page 2.

International experience suggests that it is no longer sensible to distinguish between the needs of children and adults for protection against online abuse. Online bullying and harassment can happen at all ages, and can escalate to physical violence. Accordingly, I recommend that the eSafety Commissioner's remit should be extended to cover all adults experiencing cyber-bullying so that all children and all adults experiencing online abuse problems of a serious nature are within her remit, and that the Government provide additional resources and increased staffing resources (and ASL) to support the extended function.

Information Disclosure and Delegation

The eSafety Commissioner has proposed in her submission to this review a number of clarifications to her powers and functions (lifting constraints on her ability to disclose information in relation to adults; expanding her powers to collect, use and disclose personal and sensitive information to a level commensurate with other comparable agencies; and broadening her powers of delegation to contractors and consultants), which make practical sense in order for her to be able to perform her functions effectively.

As indicated earlier, I would add enhanced data collection into this remit to enable the eSafety Commissioner to collect a full range of data from industry so that she may accurately assess the extent of the ongoing online safety challenge and the effectiveness of monitoring and compliance arrangements.

The terms of reference required me to consider whether the eSafety Commissioner might delegate some of her functions under section 64. Such an arrangement might enable a body akin to New Zealand's Netsafe to be established. I am not convinced that there is a need for the eSafety Commissioner to delegate some or all of her functions to a body corporate. Such a move would have the potential to further fragment an already fragmented sector at the very time when consolidation is needed. It would potentially split what is a reasonably coherent take-down system by adding another layer of administration which isn't necessary in this country. I don't think that it would improve on current arrangements for rapid take-down of cyber-bullying and other material, and I fear that it might worsen arrangements by potentially imposing costly and time consuming court-based procedures, and lengthening the time taken for cyber-bullying material to be removed.

Governance

I was asked to consider whether the current governance structure and support arrangements for the eSafety Commissioner provided by the ACMA are fit for purpose, and whether legislative change is required to allow the Commissioner to perform her functions and powers more effectively.

The eSafety Office was formed after the Abbott Government came to power when issues of fiscal restraint and agency consolidation[55] were very prominent on the Government's agenda. Consistent with this, the Government decided to incorporate the eSafety Office within the ACMA where the umbrella legislation for online safety then sat—the *Broadcasting Services Act*. With the very best of intentions, the Government put in place a special purpose vehicle to ring fence the funding base for the eSafety Commissioner and avoid leakage to other parts of the ACMA.

[55] As part of the Government's Smaller Government Agenda.

The result is that the Office receives funding through a special account administered by the ACMA for the purposes of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act). The ACMA submission describes this arrangement*:*

> *"Under the PGPA Act, the Chair of the ACMA is the Accountable Authority who is required to administer funding provided to the ACMA in accordance with that Act and this includes ACMA's funding for the operations of the Office of the eSafety Commissioner.*
>
> *The Chair of the ACMA is only able to delegate the ability to commit or spend public money to an 'official' (section 13 of the PGPA Act) and the eSafety Commissioner does not meet the definition of an 'official'. Accordingly, the Accountable Authority responsible for committing and spending any eSafety Office funding*[56] *is the Chair of the ACMA not the eSafety Commissioner.*
>
> *…[t]he eSafety Act sets out arrangements whereby the eSafety Commissioner is unable to directly exercise powers in relation to….staffing and administrative support….These [arrangements] entail inherent risks, inefficiencies and complexities for both parties…*
>
> *In relation to all eSafety Office staff and contractors, except for the eSafety Commissioner, they are employees of the ACMA over which the Chair of the ACMA has responsibility as the Agency Head under the Public Service Act 1999."*[57]

Beyond the ring fencing arrangement's clear success in its primary objective to secure and protect the budget of the eSafety Commissioner's function, the arrangement has not worked well at the operational level.

This is because even the most co-operative and collaborative relationships between the key players to try to make the arrangement work would not be able to override the complexity of the legislation which gives the eSafety Commissioner and the ACMA Chair responsibilities and powers which conflict. It is highly problematic that efficient administrative practice is reliant in these circumstances on the good will of the parties towards the arrangement.

The practical reality is quite different. The ACMA resisted the establishment of the Office from the beginning and, except for one short period, relationships between the various Chairs of the ACMA and eSafety Commissioners have been poor, with both understandably keen to take full responsibility for their domains. I do not see this changing in the foreseeable future.

I found in this review that the special purpose vehicle has introduced such a level of bureaucratic intervention, oversight and red tape that it is mystifying how anyone other than the most seasoned of public servants could operate effectively in this environment. This is because:

- the eSafety Commissioner is outside the *Public Service Act* and the PGPA Act, so the responsible authority to allocate staffing resources rests with the Chair of the ACMA, while both parties appear to have some, albeit disputed, responsibilities for allocating funds, the main responsibility lies with the Chair as the accountable authority; and
- there is constant confusion and differing opinion about how the special account arrangements are to operate in practice.

[56] However, the eSafety Commissioner does have her own powers for committing and spending money for contracts, so this is not the complete story.

[57] ACMA submission, page 8.

These problems have plagued the eSafety Office and the ACMA since they were introduced in 2015 and continue to this day with each extension of the Office's functions. Each new activity requires legal advice and agreement about how the financials will work and, as recently as during this review, there was even a dispute about whether the eSafety Commissioner has authority to enter into contracts involving the expenditure of monies directly, despite it being clear that she had the power under section 60 of the *Enhancing Online Safety Act 2015*.

To make the relationship have a chance of working within the ACMA, the Chair proposed that online safety functions could be fully incorporated within the ACMA[58], with the eSafety Commissioner becoming a full-time member of the Authority with a focus on online safety. This is similar to the arrangements within the ACCC for small business matters. However, I doubt very much that this would improve matters, as the eSafety Commissioner would become directly accountable to the ACMA Chair, reducing the eSafety Commissioner's independence, and distracting her from her focus on online safety.

It would be better to take the online safety functions out of the ACMA. This has the important advantage of providing the eSafety Commissioner room for a clear focus on the Government's online safety objectives, without the distraction of administrative complexities and disputes. It would enable the eSafety Commissioner to oversee the new proposed online safety legislation and consolidate online safety functions in the one domain, whilst also building more co-operative arrangements with other jurisdictions, NGOs and community organisations operating in the field. It would also be very timely to make such a change in light of the burgeoning online and digital industry.

There are several ways that this separation could be done. The first is to establish a standalone online safety agency. The second is to establish an online safety agency with corporate support services available through the Department of Communications and the Arts. The third is to incorporate the function into the Department of Communications and the Arts, but retain the eSafety Commissioner and delegate her staff and administrative responsibilities within the Department. I have also considered a fourth option, which would be to move the online safety function to the Department of Home Affairs, but I do not think this is a sensible or feasible option in view of the online safety focus on prevention, education and behavioural change rather than enforcement, security and policing.

For any of the three possible alternative models to work, the eSafety Commissioner would need to become subject to the PGPA Act and *Public Service Act*. In models one and two, the eSafety Commissioner would be declared an agency head under the *Public Service Act*, and the accountable authority under those acts, as well as receive her own appropriation funding directly. There would be no need for a special account, nor would the PGPA Act require a board as online safety is primarily a regulatory rather than a commercial function. In model three, the Departmental Secretary would delegate powers over staffing and funding for the online safety function to the eSafety Commissioner, and a new discrete online safety outcome would appear in the Department's budget papers representing the eSafety Commissioner's responsibilities.

The eSafety Commissioner argues in her submission that the eSafety Office's expanding remit, unique leadership and coordination role, and increased citizen facing services, suggest that an independent standalone office be established (model one). This would give the Commissioner greater autonomy and accountability in managing staff and funding. Some organisations making submissions to this review also saw merit in giving the eSafety Commissioner more independence, including the power to directly hire staff and delegate to anyone, including contractors.

[58] ACMA submission, page 9.

Model two would provide the eSafety Commissioner with the support that she needs to do her work on a relatively inexpensive basis, whilst also ensuring that Departmental Audit and Risk Committee controls, financial services and human resources functions and the associated corporate requirements are provided centrally on her behalf by the Department.

Even though the eSafety Commissioner would prefer complete independence from both ACMA and the Department, I am not yet convinced that this is merited. The risks are too great.

It is certainly the case that the eSafety Commissioner has high expectations that more and more resources will be directed to online safety. At the same time, there are public demands for more money to be given to the prevention of child abuse and to support youth mental health. There comes a time when an intense focus on online safety isn't sustainable because other government work is important too. There will always be competing demands around priorities to protect children from harm.

A sound relationship with the Department of Communications and the Arts as envisaged under model three would assist the eSafety Office to bed down standard public service practices; plan, prioritise and appropriately justify its resource demands; and focus on its core online safety remit at this important juncture in online safety regulatory development. It should also facilitate the rebalancing of office staffing between ASL caps and consultants, and enable more senior level coaching, training and development in mainstream public sector practice.

The creation of a separate outcome for the functions of the eSafety Commissioner would allow the funding and performance reporting associated with the Commissioner to be delineated and support the Commissioner's independence in exercising legislative powers and functions. The eSafety Office would continue to operate independently, rather than become another division in the Department. This would allow it to be seen to exercise online safety leadership. It would also allow easy transition to a standalone entity should that be found by the Government to be appropriate (as resourcing would be ring fenced and easily identifiable) in the event that the function continues to grow and the requirements of managing a public sector entity are met.

By operating within the policy department, the eSafety Commissioner would be part of the policy making environment—delivering a stronger focus to the policy debate and providing more centralized control of online policy issues which currently stretch across a number of different portfolios. The eSafety Commissioner would have more opportunities to collaborate inside and outside government. She would also be able to tap into the stakeholder relationships established and maintained by the Department which will facilitate stronger collaborative arrangements between the eSafety Commissioner and others thereby ensuring that online safety standards are more likely to be robust, reasonable and effective.

I recommend that the role of the eSafety Commissioner and her Office be undertaken within the Department of Communications and the Arts, with the Office's ASL allocation along with its resources, consultants and programs be moved to the Department and the ACMA allocations be reduced accordingly. I further recommend that a review of the governance arrangement be undertaken after a 3 year period of transition to determine the possibility of setting up a new standalone agency, based on the scope and level of demand for the online safety function and the level of maturity of the Office's operations.

Regulatory regimes

In considering the most effective balance of tools available for dealing with prohibited and harmful online content, I took account of the Department of Communications and the Arts 2014 work on regulation[59]. Their publication provides the following regulation overview:

- Black letter law is appropriate where there is a compelling reason for regulation—usually required to protect the public or industry from harm and where enforcement measures are necessary in case of non-compliance. It is often used to deal with monopoly behaviour or anti-competitive practices.
- Co-regulation is where an industry develops its own code or accreditation scheme that has legislative backing, including government enforcement. Co-regulation is appropriate where the industry has high visibility of the problem, can manage the problem itself, and is willing to disclose information in addressing the problem. Co-regulation works best when homogenous products are provided by a small number of players.
- Self-regulation is where an industry voluntarily develops, administers and enforces its own rules and standards without any formal government oversight or legal backstop for enforcement. It usually does so under threat of possible government legislation or to raise industry standards.

Submissions to the reviews highlight community perceptions that not enough is being done for online safety, on the one hand, and industry concerns that they should not be tied up in unnecessary red tape when, in their view, the self- and co-regulatory approaches are working and remain the most effective and efficient approach to online safety, on the other hand.

The extent to which industry is actually blocking or taking down illegal material proactively is difficult to say in the absence of publicly available data about blocking and content removal. However, I have no reason to dispute the validity of the arguments made throughout these reviews that Australian industry appears to have voluntarily acceded to the Government's policies and has blocked or taken down illegal material.

DIGI's submission[60] to this review outlines the way industry has become increasingly sophisticated at using technology to increase users' safety online in addition to the existing reporting and blocking technologies that have existed for many years, and their members' system of notice and take-down processes which enables users to flag inappropriate content and have it reviewed by a person. DIGI correctly notes that the sheer volume of content and the need to establish context makes it difficult to proactively identify every piece of content that is in violation of their members' online safety policies. Further, it argues that the industry is striving constantly to improve and is investigating new technologies that will take their work even further, especially image hashing and machine learning algorithms[61], which have been found to be effective in proactively identifying terror-related, suicide-related and image-based content and surfacing it for referral to a person for review and removal.

[59] Department of Communications and the Arts, Policy Background Paper No 2, *Regulating harms in the Australian communications sector: Observations on current arrangements*, May 2014.

[60] DIGI submission, pages 2-3.

[61] Image hashing works by taking a fingerprint or "hash" of the image that is then used to prevent it appearing elsewhere on the internet, while machine learning algorithms identify potentially problematic content before many people have viewed it and then triggers a human review.

The reasons for industry doing so are not simply to make the internet a safe and respectful place where people have positive experiences and make meaningful connections. It is also likely that the reasons relate to the level of community concern about child abuse, violent and disturbing pornography or incitement to terrorism; the desire of industry to act in line with community expectations; and reputational risk if they fail to do so. Pointing to voluntary action by social media companies has also been a key argument to resist regulation on the basis that government intervention is unnecessary.

Despite this commitment, I started to hear towards the end of my reviews anecdotal evidence to the effect that, in reaction to increasing government pressure for more online industry preventative action across a number of different environments (but notably copyright, security and privacy), some parts of the industry have taken a step back to again doing just the basics of compliance with the current minimal safety requirements of the legislative framework. The lesson to be drawn from this is that the level of industry commitment to online safety is fragile and unreliable, and needs to be shored up by being given a legislative basis.

By and large, declining rates of public trust and rising levels of outrage are strong indicators that the Australian community's hopes have been shattered in terms of their belief that people, industry and businesses will exhibit conduct at a level commensurate with community expectations. The dilemma facing society is that people no longer feel that they can rely on industry, business or even the church to do the right thing, let alone individuals working within the system.

The social license to operate of some business sectors, many companies and institutions is being increasingly challenged as the community demands higher standards which better reflect their expectations of good behaviour and appropriate practice. It should therefore come as no surprise to the online industry that the tide of change is against it—with the community calling on the Government to provide higher levels of intervention to control and penalise misconduct online, whether it be malfeasance or neglect, and to protect Australians more generally.

Echoing these demands, Ministers from Australia, Canada, New Zealand, the UK and the USA recently issued a Ministerial Statement and a Communique on countering illicit use of online spaces:

> *"… [We] reiterate our determination…to ensure our response is commensurate with the gravity of the threat. Our citizens expect online spaces to be safe, and are gravely concerned about illegal and illicit online content….We stand united in affirming that the rule of law can and must prevail online."* [62]
>
> *"… The anonymous, instantaneous, and networked nature of the online environment has magnified…threats and opened up new vectors for harm….Governments have a responsibility to protect those within our borders against both physical and digital threats, and to ensure that the rule of law prevails online, as it does offline. … [The digital industry needs to] take more responsibility for content promulgated and communicated through their platforms and applications."*
>
> *"… We call on industry to meet public expectations regarding online safety by:*
>
> - *developing and implementing capabilities to prevent illegal and illicit content from ever being uploaded, and to execute urgent and immediate take-down where there is a failure to prevent upload;*
> - *deploying human and automated capabilities to seek out and remove legacy content;*

[62] Five Country Ministerial 2018, *Joint Statement on Countering the Illicit Use of Online Spaces*, 28–29 August 2018, page 1, www.homeaffairs.gov.au/about/national-security/five-country-ministerial-2018/countering-illicit-use-online-spaces.

- *acting on previous commitments to invest in automated capabilities and techniques to detect, remove and prevent re-loading of illegal and illicit content, as well as content that violates the company's terms of service;*
- *prioritising the protection of the user by building user safety into the design of all online platforms and services, including new technologies as they are deployed;*
- *building on successful hash sharing efforts to further assist in proactive removal of illicit content;*
- *setting ambitious industry standards, and increasing assistance to smaller companies in developing and deploying illicit content counter measures;*
- *building and enhancing capabilities to counter foreign interference and disinformation;*
- *preventing live streaming of child sexual abuse on all platforms."* [63]

It is therefore quite understandable that in the online safety area, the co-regulatory system in Australia is increasingly shifting more towards black letter law, with each and every new legislative amendment as more and more issues emerge online that the Government considers require further protections to prevent harm. Coupled with the fact that social media and other forms of digital communication and applications are increasingly the basis for many everyday social interactions between people and for doing business, it is hard to imagine that light touch regulation of the sector can be sustained for much longer.

The challenge of multiple applications across and beyond social media mean that industry will struggle to manage the problem itself, as demonstrated by the ongoing effectiveness challenges of the current industry codes. The relative ease with which the online world can deliver harm on a wide scale, along with the constantly increasing number of players, platforms and devices which make visibility of the perpetrators difficult and magnify the potential for avoiding detection, are factors that make Government intervention in this market necessary and inevitable in order to protect end-users from harm.

The absence of data disclosing industry's online safety activity and the refusal of major social media companies to agree to participate in a scheme designed to facilitate voluntary compliance with removal requests from the eSafety Commissioner under cyber-bullying arrangements, together with industry's continuing resistance to further online safety regulation here and overseas, point to the need for stronger legislation.

We know that co-regulation works best when homogenous products are provided by a small number of players, which is certainly not what we are experiencing with the exponential increase in online opportunities. It flies in the face of the modern reality where the internet, social media and other elements of the digital age are an integral part of people's lives and workplaces, that co-regulation should continue to be the primary source of regulation of the online system. The balance needs to be moved more towards black letter law, supplemented by an updated and modernized supportive code framework.

Against this, I have heard strong arguments from industry that suggest that freedom to operate with only minimal regulation is essential for the most effective use of the technology.

[63] Five Country Ministerial 2018, *Official Communique*, 17 October 2018, pages 1–2.

Internet service providers, content service providers and platforms continue to argue that they are not responsible for the content carried on their networks and hosted on their platforms. I disagree because the mere act of facilitating distribution brings them into the system, and makes them equally responsible for the content. I also note that similar arguments from the financial services industry about them not being responsible for downstream fees, services and contracts have been blown out of the water by the Royal Commission on Financial Services.

From a practical point of view, I am conscious that all of the digital platforms have terms and conditions of use which can and should disclose to their users and purveyors of applications using their systems content that may not be carried or supported on their platforms.

The Internet Society argued in its submission to this review that *"… [u]sing internet blocking to address illegal content or activities is generally inefficient, often ineffective and generally causes unintended damages to internet users."*[64] While I accept that blocking technologies employed by platforms have had unintended consequences in the past, industry practices in recent years in this country and overseas, would suggest that they are entirely possible. Google's acquiescence to Chinese demands for blocking technology in their new Chinese Dragonfly enterprise, for example, indicates that technological developments now mean that effective blocking interventions by industry are entirely feasible and will not undermine profitability.

I am drawn to say that the view sometimes promulgated by the online industry that increased regulation will damage innovation, is complete bunkum. It is necessary only to look at the extent of online innovation and ICT start-ups in recent years to know that the lure of significant business returns and, for user-generated content, popularity measures such as retweets, likes and friends and followers, will be sufficient to maintain high levels of innovation in this intensively competitive global business market. Moreover, the purveyors of harmful and illegal material are highly creative and active innovators who are constantly challenging the detection mechanisms of governments and industry world-wide. Their business models must be broken by swift and regular action.

In the words of the 5 Nations Ministers, the rule of law can and must prevail online, as it does in the physical world.

I therefore recommend that the Government move to strengthen the regulatory framework for digital and online safety by enforcing a much more proactive regulatory regime in legislation, with additional requirements on all of the online and digital industry operating in Australia to implement measures to patrol, detect, remove and deter the posting of illegal and harmful content, and to report annually to the eSafety Commissioner on their activities, with serious penalties for non-compliance.

[64] Internet Society submission, page 4.

New legislation

Legislation governing online safety sits across two main pieces of legislation. It has been impossible in this review to discuss one without dealing with the other one. And a third source of online safety protection, the Commonwealth Criminal Code, which provides criminal penalties for some forms of image-based abuse, is entirely outside the scope of my reviews.

It is striking that these pieces of legislation provide a series of functional responses to deal with online safety issues without any core binding rationale or framework. The name, the '*Enhancing' Online Safety Act,* suggests that it is building on a solid online safety legislative framework, but I am not convinced that there is one there. Instead, what we have in legislation, especially the two Schedules to the *Broadcasting Services Act*, is a bewildering array of requirements, which are confusing, overlapping, technology-specific and often over-drawn. Added to this, I found no apparent reason to have separate pieces of legislation, other than to give authority to the eSafety Commissioner to perform her full range of functions and that is no reason to maintain them.

The majority of submitters to these reviews proposed taking Schedules 5 and 7 out of the *Broadcasting Services Act* and incorporating them within the *Enhancing Online Safety Act* after a thorough review to clean up and modernize both pieces of legislation, resulting in a single piece of legislation relating to online services and content. I support this approach most strongly and consider that the legislation should be redrawn into an integrated act which deals systemically with the challenge of online safety in its entirety.

A single piece of legislation would bring all the component parts of the Government's online safety response into one Act, comprising the functions in the *Enhancing Online Safety Act*, and Schedules 5 and 7 of the *Broadcasting Services Act*, the residual statutory review requirement in the *Enhancing Online Safety (Non-consensual Sharing of Intimate Images) Act* and any consequential legislative changes arising from my review work. This would improve clarity, reduce complexity and establish more straightforward processes for removing illegal or inappropriate or bullying content. It would enable the role and functions of the eSafety Commissioner to be clearly specified. The legislation would be known as the Online Safety Act. It would cover online abuse of both adults and children.

The new Act would incorporate objectives to describe what the legislation aims to do. Those objectives could usefully be framed around safer, positive online experiences and encompass the following:

- To promote the safety of all people who engage in online and digital communications.
- To avoid harm being done to all people engaged in online and digital communications.
- To protect children from online and digital danger.
- To drive behavioural change to minimise the incidence and reduce the severity of harmful online and digital communications.

The legislation would also include a statement of principles that would guide the regulatory approach of the eSafety Commissioner.

It would specify the roles and functions of the eSafety Commissioner, as part of the Department of Communications and the Arts, and her inclusion under both the PGPA Act and the *Public Service Act*. The special account would be abolished and the Office would be funded in the usual way through an appropriation.

The legislation would also specify that there should be a National Online Safety Plan, and that the eSafety Commissioner would be supported in her role by a standing eSafety Advisory Committee.

It would empower the eSafety Commissioner to collect data on industry online safety activity, co-ordinate online safety arrangements nationally, and disclose information more widely in the pursuit of online safety and protection from harm.

Recommendations

1. It is recommended that the Government introduce the significant and wide ranging changes to the online safety system identified in this review report, which will set out the new norms and standards for the online world, and establish new regulatory arrangements to put them into practice.
2. To bring about these changes, it is recommended that:

   (a) the regulatory framework for digital and online safety be strengthened by enforcing through legislation a much more proactive regulatory regime, with additional requirements on all of the online and digital industry operating in Australia to implement measures to patrol, detect, remove and deter the posting of and access to illegal and harmful content, enforce their own safety policies and behavioural standards, and to report annually to the eSafety Commissioner on their activities, with serious penalties for non-compliance;

   (b) a single, easy to read piece of online safety legislation be created, which will replace the existing pieces of legislation (*Enhancing Online Safety Act 2015*, Schedules 5 and 7 of the *Broadcasting Services Act 1992*, and the *Enhancing Online Safety (Non-consensual Sharing of Intimate Images) Act 2018*) and set out the core elements of the Government's online safety policy to protect Australians from online harm and illegal behaviour. The new Online Safety Act would incorporate directions set out in this report, including:

   - objectives to protect against harm and promote online safety,
   - the roles and responsibilities of the eSafety Commissioner in online safety and regulation,
   - a technology, platform, service, distribution and device neutral approach to regulation,
   - new legislative standards for a more proactive regulatory regime and toughened enforcement powers,
   - streamlined industry requirements alongside a new mandatory industry code for all industry participants with online and digital activities, with the code commencing within a year of the new legislation being enacted,
   - coverage of all Australians, including cyber-bullying coverage for all children and all adults,
   - data collection and reporting requirements,
   - new classification arrangements that focus on illegal, dangerous and harmful content, and
   - other necessary adjustments as proposed.

   The timing of the introduction of the new Act should be a high priority for Government, with the aim of it being introduced by 1 July 2019, and passed into law in the second half of 2019, subject to other legislative priorities;

   (c) a National Online Safety Plan be produced by the Department of Communications and the Arts and the eSafety Commissioner in consultation with stakeholders, to set out clearly the national online safety strategy framework, operational arrangements and implementation priorities and responsibilities. The new plan would take effect from 1 January 2020;

(d) immediate efforts be made to establish more effective collaborative partnerships and co-operative working relationships:

- across the sector, through the creation of a new standing eSafety Advisory Committee to advise the eSafety Commissioner, the Departmental Secretary and the Commonwealth Agency Heads Committee on Online Safety on best practice online safety and administration,
- between law enforcement and the Office of the eSafety Commissioner, in order to activate more effective enforcement arrangements, and
- through the introduction of a national rolling program of online safety work, which would maintain strong co-ordination and alignment across the sector.

3. To facilitate these changes, it is additionally recommended that governance arrangements be improved by moving the eSafety Commissioner and her Office (along with associated ASL, contractors, resources, programs and responsibilities) out of the Australian Communications and Media Authority and into the Department of Communications and the Arts. Under this arrangement, the eSafety Commissioner would retain the independence of her office in a new departmental online safety stream of business and assume responsibility for a new departmental online safety outcome, all of her staff and resources, and be brought under the *Public Service Act 1999* and the *Public Governance, Performance and Accountability Act 2013*, with the special purpose vehicle being abolished.
4. It is further recommended that these new governance arrangements be reviewed after a transition period of 3 years to assess the possibility of setting up a new standalone online safety entity.
5. It is also recommended that the resources and average staffing level of the Office of the eSafety Commissioner be boosted to support the proposed new and expanded functions envisaged in this report.