

Submission of the Department of Home Affairs

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

1 August 2018

***Introduction***

Online child abuse, technology-facilitated abuse and cyberbullying are complex issues requiring a comprehensive Government response that is interconnected and utilises preventative and educative approaches, strong engagement and cooperation, as well as robust civil and criminal enforcement measures for the most serious cases. Government responses to these online safety issues take a whole-of-government approach, integrating activities at both Commonwealth and state and territory levels, and strong engagement with industry and the non-government sector.

The Office of the eSafety Commissioner (eSafety Office) is supported by and empowered under the *Enhancing Online Safety Act 2015* (Online Safety Act)and Schedules 5 and 7 of the *Broadcasting Services Act 1992* (Online Content Scheme) to achieve the functions outlined in section 15 of the Online Safety Act and section 94 of the Online Content Scheme. The eSafety Officeplays an important and valuable role in this holistic model.

The Department of Home Affairs (the Department) holds policy and enforcement responsibilities for aspects of online safety matters, including:

* policy responsibility for a broad remit of online criminal conduct, including offences for online child abuse in the Commonwealth *Criminal Code Act 1995* (Criminal Code), criminal cyberbullying, and technology-facilitated abuse;
* countering offensive online content, including terrorist material;
* cyber security; and
* the framework by which law enforcement and intelligence agencies can access telecommunications information for criminal and national security purposes.

The Australian Federal Police (AFP) has functions that intersect the eSafety Office’s focus and remit. The AFP is responsible for aspects of online safety education and community engagement, in addition to its role in the investigation and enforcement of online crime. The AFP delivers the ThinkUKnow program in schools throughout Australia to educate children, parents and teachers about online safety. This submission incorporates input from the AFP, as well as other relevant Home Affairs portfolio agencies.

The Australian Criminal Intelligence Commission (ACIC) manages the Australian Cybercrime Online Reporting Network (ACORN) which provides a mechanism to report online crimes and abuse to law enforcement, including prohibited online content, cyberbullying, and online sexual activity with children such as grooming, procuring, and live-streamed child abuse.

The Commonwealth Transnational Serious and Organised Crime Coordinator (TSOC Coordinator) aims to strengthen the national effort to combat the serious and rapidly evolving threat posed by transnational, serious and organised crime. Combating child exploitation, including child sexual abuse material, is one of the Coordinator’s immediate priorities.

The Department’s submission to the *Enhancing Online Safety Act 1995* and Online Content Scheme reviews (the Review) will focus on the matters which interact with the Home Affairs portfolio’s responsibilities, and will not comment on the support arrangements, staffing, funding, and governance structure of the eSafety Office.

***The role of the Office of the eSafety Commissioner – functions and powers***

The Department considers that the Online Safety Act and Online Content Scheme provide appropriate powers and functions in support of the eSafety Office’s mandate to enhance online safety for Australians.

The Department does not consider legislative change to the Online Safety Act is required for the eSafety Office to continue to effectively deliver on its functions and responsibilities. However, if legislative reform results from the Review, the Department suggests the Review consider, in particular, the role of the eSafety Office in relation to social media providers and accessibility of terrorism content.

The Department considers the eSafety Office is successful in exercising the duties and functions of the role under the current legislative regime. The Department supports improvements to the processes and policies by which the eSafety Office works with the Home Affairs portfolio and across broader government and non-government entities who play a role in Australians’ online safety.

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 (noting some of these powers and functions are subject to Parliament passing the Enhancing Online Safety (Non‑Consensual Sharing of Intimate Images) Bill 2018). The functions and responsibilities of the eSafety Office are a strong complement to the criminal justice approach led by the Home Affairs portfolio.

The eSafety Office’s civil enforcement measures and recourse options, such as its work to remove reported cyberbullying material, are extremely valuable additions to the criminal justice responses led by the Home Affairs portfolio. The eSafety Office’s remit to address cyberbullying of Australian children is particularly valuable, where law enforcement responses to complaints that may not meet a criminal threshold, or primarily involve the conduct of children, are less desirable and appropriate. The eSafety Office’s role to address and resolve complaints of cyberbullying and image-based abuse helps to reduce strain and pressure on the criminal justice system, and provide timely outcomes for victims of online abuse.

*Expanded role of the eSafety Office*

The Department acknowledges the high quality resources and initiatives undertaken by the eSafety Office as part of their broadened remit to address issues affecting adult Australians. The eSafety Office has demonstrated an unwavering commitment to empowering all Australians to have safer, more positive experiences online.

The Department strongly supports the further expanded role of the eSafety Office to administer a civil prohibition and penalty regime, and associated take-down powers, for the non-consensual sharing of intimate images. The eSafety Office’s online reporting portal for image-based abuse and the eSafety Women website, containing resources to educate and support victims of technology-facilitated abuse, are valuable initiatives toward enhancing online safety for all Australians. The proposed complaints and objections system for victims of image‑based abuse in the Enhancing Online Safety (Non-Consensual Sharing of Intimate Images) Bill 2018 would be a valuable initiative making further enforcement options available to victims of image‑based abuse.

The role of social media platforms in both our economy and society is increasing in both importance and influence. As a result, the number of Government interactions with social media platforms is growing, both on a regulatory and cooperative basis. A significant number of these interactions occur within the Home Affairs Portfolio, including work on cybercrime, the take down of violent extremist propaganda, countering foreign interference and mitigating threats to our democratic processes.

The Review should consider the increasingly relevant leadership role of the eSafety Commissioner in supporting whole-of-government engagement with social media platforms, and the best way to enhance and support this role in the future.

Finally, the eSafety Commissioner’s website outlines research that found 33 per cent of young Australians have seen videos or images that promote terrorism. The Department submits that if any legislative reforms are considered, they support the eSafety Office’s ability to limit the accessibility and availability of this content, as well as undermine its appeal with young Australians.

***Recent relevant inquiries and reviews***

*The cyberbullying inquiry*

In March 2018, the Senate Standing Committee on Legal and Constitutional Affairs reported on its ‘inquiry into the adequacy of existing offences in the Commonwealth Criminal Code and of state and territory criminal laws to capture cyberbullying’. The report found that prevention, community engagement and education measures to combat cyberbullying are vital to countering this complex issue. The Government’s response to the recommendations of this inquiry is pending.

*The Royal Commission into Institutional Responses to Child Sexual Abuse report recommendations*

The Review discussion paper refers to recent reviews relevant to the functioning of the eSafety Office. The Department draws the Review’s attention to the recommendations of the Royal Commission into Institutional Responses to Child Sexual Abuse.

The Royal Commission into Institutional Responses to Child Sexual Abuse makes a number of recommendations that relate to the functions of the eSafety Office. Specifically, recommendations 6.2 and 6.19 to 6.24 are relevant to the functioning of the eSafety Office and should be considered as part of any legislative or policy reform resulting from the Review.

***General principles***

*Technologically neutral legislation*

The Department submits that any legislative reforms resulting from the Review should be framed in a way that is neutral to technology. Technologically neutral legislation, policy, and procedure provides a best practice model to maintain relevance and adapt effectively to the quickly shifting online environment. As technology evolves, the behaviours and uses of that technology continue to expand. For the eSafety Office to remain relevant and effective in the face of new and emerging technology, legislation, policy and procedure should be future‑proofed. This is particularly relevant to the definitions of prohibited online content and the way legislation refers to existing and emerging platforms and methods of communication.

We also note that technological advancements, and in particular the prevalence of encryption networks and the ‘dark web’, are making it more challenging to detect and disrupt the propagation of child abuse material. Any changes to the Online Safety Act or Online Content Scheme should consider the future state of cyber communication, not just the current state.

Any legislative reform undertaken as a result of this review should consider the Department’s interests as policy leads on related offences in the Criminal Code. This is particularly relevant to any definitions in either the Online Safety Act or Online Content Scheme that interact with offences in the Criminal Code. For example, definitions of prohibited content and definitions of child abuse material should be aligned, as well as definitions of services and/or platforms to which regulations apply.

The Department further notes that the Department of Communications and the Arts will be consulting on how to modernise the National Classification Scheme through a separate discussion paper. The Commonwealth Transnational, Serious and Organised Crime Centre should be consulted during this process, with relation to National Classification Scheme categories to identify prohibited content sufficiently, in a way that is adaptable to new types of content that may emerge in the online environment.

***Online safety education***

*AFP’s ThinkUKnow program*

The Review discussion paper refers to the eSafety Commissioner as the ‘lead agency to coordinate and lead online safety activities across Australia’. The Department notes the language in the Online Safety Act, which references the eSafety Office’s role to ‘coordinate’ online safety activities. The Department draws the Review’s attention to online safety initiatives that are led by AFP, where the eSafety Office does not have a lead or coordinating role, and recommends an approach to the eSafety Commissioner’s role that recognises the remits of other stakeholders.

AFP participates in targeted events to increase online safety awareness, particularly with relation to the safety of children, and also administers the ThinkUKnow program.

ThinkUKnow uses police operational awareness and understanding of online safety trends to tailor programs to youth (school aged children from prep/kindergarten through to Year 12), parents, carers and teachers. ThinkUKnow has been running nation-wide for nine years through a network of trained volunteers and representatives from all state and territory police forces.

ThinkUKnow complements education initiatives coordinated by the eSafety Office, and represents an example of a best-practice holistic approach to online safety education and awareness raising.

AFP engages with the eSafety Office about the ThinkUKnow program, providing an opportunity to review and make comment on presentations and resources, with the aim of ensuring consistent messaging between eSafety Office initiatives and AFP resources, as far as possible. ThinkUKnow refers to eSafety resources and capabilities, wherever relevant.

AFP will continue to engage with the eSafety Office for online safety awareness-raising opportunities, and supports strong engagement with the eSafety Office to enhance current initiatives and partnerships to effectively deliver on the eSafety Office’s mandate.

***Partnerships with the eSafety Office***

*Commonwealth Transnational Serious and Organised Crime Coordinator and Australian Centre to Combat Child Exploitation*

The TSOC Coordinator is responsible for overseeing the implementation of the Australian Centre to Combat Child Exploitation (ACCCE). The ACCCE was recently established to drive a national effort to combat the global epidemic of child exploitation, both here and overseas. It will combine the resources of the various agencies in the Home Affairs portfolio, and link to other Commonwealth departments, state agencies and, importantly, non‑government organisations with expertise in dealing with child sexual abuse and exploitation, its victims and consequences. The Department recommends that the eSafety Commissioner continue to work closely with the ACCCE to combat child sexual abuse and exploitation.

*Information sharing and cooperation with law enforcement agencies*

The eSafety Office’s powers for referral and information sharing under the Online Safety Act and Online Content Scheme are vital to the ability of the eSafety Office to refer all online child abuse material and the most serious instances of cyberbullying and technology-facilitated abuse that reach a criminal threshold, to appropriate law enforcement agencies. These powers and functions should be maintained through any legislative reform that might take place as a result of this Review.

AFP frequently refers enquiries to the eSafety Office and their website, particularly in relation to the eSafety Office’s reporting mechanisms for image-based abuse and cyberbullying, but also in relation to online safety matters which fall more comfortably within the eSafety Office’s roles and responsibilities and are outside of the remit of the AFP or state or territory law enforcement. This is particularly relevant to instances of cyberbullying between children, or self-generated sexual images of children where a law enforcement approach is not always the most appropriate course of action.

*Referrals from the eSafety Commissioner to Australian law enforcement for criminal matters*

Close cooperation with law enforcement is an essential process by which the eSafety Office can effectively fulfil its functions and deliver on its mandate to enhance online safety.

The Online Safety Act allows the eSafety Office to work closely with Australian law enforcement agencies to disclose information and refer matters of a sufficiently serious nature for criminal investigation. These processes are important to ensure that matters which fall within the remit of AFP and other law enforcement agencies can be dealt with according to the powers and functions of those law enforcement agencies. Where a matter has reached the threshold of criminality, the eSafety Office can refer it to AFP or a relevant state or territory law enforcement agency under section 80 of the Online Safety Act for investigation and potential prosecution. The Australian Government supports improving the process for identifying and referring matters which reach this criminal threshold to AFP and other law enforcement agencies.

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 material, which may form part of a complaint to the eSafety Office for cyberbullying or image‑based 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. This might be supported by closer working relationships such as secondments, that would allow the use of police powers while jointly investigating criminal offences that benefit both authorities.

In May 2018, as a consequence of a recommendation of the Senate Standing Committee on Legal and Constitutional Affairs’ ‘inquiry into the adequacy of existing offences in the Commonwealth Criminal Code and of state and territory criminal laws to capture cyberbullying’, AFP proposed the eSafety Office second a staff member into AFP’s Child Protection Assessment Centre. An eSafety Office secondee may bring AFP powers to bear in defined investigations and pending information sharing arrangements being appropriately determined. This remains an option for closer cooperation between the eSafety Office and AFP. AFP will also continue to closely engage with the eSafety Office in relation to a number of referrals received through the AFP Child Protection Assessment Centre.

***eSafety Office’s enforcement powers***

The eSafety Office’s ability to work with social media services to remove content under the Rapid Removal Scheme, or to utilise enforcement mechanisms such as the End-user Notice Regime, complements the role of the eSafety Commissioner to develop and maintain strong and effective partnerships with content hosts and platforms for the voluntary take down of such material.

The eSafety Office’s enforcement powers, such as the cyberbullying complaints scheme, the Rapid Removal Scheme, and the End-user Notice Regime are important to protecting children from content on social media. The Department understands that, of over 700 cyberbullying complaints received since the launch of the eSafety Office, all have been resolved informally within a short timeframe. The Department considers this demonstrates the success of the eSafety Office’s role to develop relationships with social media providers and advocate for the protection of Australian children from the harm caused by cyberbullying material on large social media sites. The Department understands that the tiered model, and the eSafety Office’s responsiveness to requests from the public to remove material, has reduced the impact of cyberbullying.

*eSafety Office’s access to data*

The Department notes that the eSafety Office generally obtains information and data directly from victims or from service providers, including social media providers overseas, through voluntary disclosure. The framework by which the eSafety Commissioner is able to make requests of over-the-top service providers to administer its civil regime and conduct investigations into non-criminal instances of cyberbullying are adequate and proportionate, considering the broader regulations for access to data.

A number of measures could enhance voluntary disclosure and assist the eSafety Office in applying its enforcement functions, where it is appropriate to do so. These measures include information sharing arrangements, and effective and close partnerships with law enforcement.

AFP notes that the eSafety Office may be encountering issues under the End-User Notice Scheme when issuing end-user notices without access to specific data. Difficulties may include identifying perpetrators to apply its End-User Notice Regime through the use of public record. AFP notes that these difficulties are shared across law enforcement, even when pursuing more serious criminal matters. The AFP recommends partnerships between the eSafety Office and law enforcement to alleviate this issue in certain circumstances, such as criminal investigations. The Department does not consider this an issue that will be able to be resolved through legislative reform.

The success of the eSafety Office in applying enforcement capabilities as outlined in the Online Safety Act is directly linked to its ability to develop relationships and efficient processes between the eSafety Office and platform providers, to achieve good outcomes with requests for voluntary non-content data.

*Terrorist material*

The Department is aware that data hosted overseas can present challenges with relation to terrorist material online. The eSafety Office powers to issue take down notices to remove material that advocates the doing of a terrorist act only applies to content hosted in Australia. However, if the content is hosted overseas – common in the case of terrorist material – the eSafety Office cannot issue a takedown notice.

Compared to other types of content, such as child exploitation material, there are no established channels of international cooperation regarding terrorist material. While there are mechanisms for Australia’s Classification Board to refuse classification of content, including overseas hosted pro-terrorism content, this is unlikely to be effective due to difficulties in enforcing these decisions regarding overseas content and the timeframes of this process.

***Delegation of the eSafety Commissioner’s powers and functions***

The Department notes without comment the ability for any or all of the eSafety Commissioner’s functions to be delegated to Australian Communications and Media Authority (ACMA) staff above the classification APS 6.

The eSafety Commissioner’s delegation power under section 64 of the Online Safety Act specifically excludes the ability to delegate powers under section 35 and 37 with relation to powers to issue social media notices and formal warnings. These exceptions are sensible, and more broadly the Department recommends against the delegation of any enforcement powers the eSafety Commissioner possesses or may come to possess should legislative reform be undertaken as a result of these reviews.

Furthermore, any delegation made under section 64 of the Online Safety Act powers should be only undertaken having regard to the privacy of the persons involved, especially with regard to cyberbullying, which can often relate to children. If a section 64 delegation was to be made, the delegate should be well aware of its obligation to refer such matters that fall within the purview of law enforcement, especially with relation to online child abuse material.

***Online Content Scheme and prohibited content online***

The Department notes that a number of Commonwealth Acts and Regulations rely upon or extrapolate the definitions and concepts set out in Schedules 5 and 7 of the Broadcasting Services Act 1992. For example, relevant to the Home Affairs portfolio, the Criminal Code and *Telecommunications (Interception and Access) Act 1979* may be significantly impacted by any legislative reform of the Online Content Scheme. Any legislative reform should involve consultation across all affected portfolios.

The Department also notes the technology-specific language used throughout the Online Content Scheme, and, if this review were to result in legislative reform, refers the Review to the Department’s comments outlining the advantages of technologically-neutral language above.

The definitions of prohibited content in Schedule 7 of the Online Content Scheme rely heavily upon the National Classification Scheme. Given the decreasing connection between traditional media falling under the National Classification Scheme and online platforms for communication and information dissemination, there may be scope to update the way prohibited content is defined in the Online Content Scheme.

***Industry codes***

Industry codes that provide for filtering or controlled content can be a helpful tool to protect children from harm online. However, AFP believes that a combination of technical and behavioural actions is required to ensure that children and young people have safe online experiences. AFP advocates an approach which continues to empower parents and carers to implement behavioural actions, in conjunction with technical options such as filtering software, should this be appropriate for their family circumstance.

Some parental controls and monitoring software can be beneficial to ensure safe searching for younger children, and may help ensure that only appropriate content is viewed. However, parental controls and software vary significantly in what they can or cannot monitor. Filters risk creating a false sense of security, and may also block content that is not actually inappropriate, but may still let potentially harmful content through.

It should also be noted that filtering software may not necessarily prevent unwanted contact or approaches to children made through apps and games. AFP’s ThinkUKnow program aims to educate parents, carers and children on the behavioural actions that can be implemented to address this.

As young people become more aware and increase their digital knowledge and literacy, they will often be able to subvert controls and filtering software, resulting in more complex challenges than not having any technical controls or filters at all. The AFP encourages parents and carers to ask themselves what they want to achieve and research the products that best suit the individual needs of their family, noting there is no ‘one size fits all’ approach.

Contact Officer:

Andrew Warnes, Assistant Secretary National Security Policy Branch, the Department of Home Affairs

(p)

(e)

(a) PO BOX 25, Belconnen ACT 2616