File No.: 18/1891#6

March 2018

**Subject: The future of content regulation and Freedom of Expression in the Digital Age roundtable**

The Australian Government has the pleasure to provide the following information to assist in the preparation of the Special Rapporteur on Freedom of Opinion and Expression’s report to the UN Human Rights Council on online content regulation as part of his multi-year examination of Freedom of Expression and the Private Sector in the Digital Age.

**Introduction**

Australia believes that human rights, including the right to freedom of expression, should be protected online as they are offline. The Australian Government supports an open, free and secure internet where people can freely access information and express their ideas. We believe that the maintenance of security online and the protection of freedom online reinforce each other. A secure cyberspace provides trust and confidence for Australians, and underpins freedom of expression and reinforces safe and vibrant communities.

Australia’s International Cyber Engagement Strategy, launched in October 2017, recognises the breadth of cyber issues and contains a dedicated chapter on human rights and democracy online. In this chapter, Australia commits to advocate for the protection of human rights and democratic principles online; support international efforts to promote and protect human rights online; and ensure respect for and protection of human rights and democratic principles online. Under the Strategy, the Government is supporting NGOs that defend human rights online, including the Freedom Online Coalition and the Digital Defenders Partnership. Through its Cyber Cooperation Program, Australia is also funding capacity building efforts in the Indo Pacific to increase states’ awareness of their human rights obligations online. The Government will also ensure respect for human rights and democratic principles are considered in all Australian Aid projects that have a digital component.

At home, Australia has developed a carefully balanced regulatory system to ensure that Australians’ freedom of expression and opinion are respected, while also regulating the darker elements of the internet in a targeted, measured and defensible way.

The Government only intervenes online in limited areas to enhance children’s safety and filter, block or ‘take down’ content relating to serious criminal activity (e.g. content that represents an incitement to violence, terrorist-related material, child exploitation and child sexual abuse). We recognise there a number of online risks that can cause harm to both adults and children, and that proper controls need to apply to social media and content services to ensure individuals can seek redress, advice and support. We work with the private sector, including social media organisations, to promote corporate responsibility for a safe, open and secure internet.

All Bills and legislative instruments introduced into the Australian Federal Parliament must be accompanied by an assessment of the bill’s compatibility with the rights and freedoms recognised in the seven core international human rights treaties that Australia has ratified. The Parliamentary Joint Committee on Human Rights (PJCHR) also examines and reports on the human rights compatibility of all bills and legislative instruments considered by Parliament. The Government regularly reviews its laws to ensure they remain reasonable, necessary and proportionate with respect to limitations of rights.

To inform the High Commissioner’s report on this occasion, the Government is pleased to provide the following further information on its content regulation framework.

**Online Safety Issues (Cyberbullying, image-based abuse and prohibited content)**

* The Office of the Children’s eSafety Commissioner (eSafety Commissioner) was established in July 2015[[1]](#footnote-2) to take a national leadership role in online safety for children. Legislation came into effect on 23 June 2017 which expanded the remit of the Commissioner to address online safety issues affecting all Australians. Section 15 of the *Enhancing Online Safety Act 2015[[2]](#footnote-3)* specifies the broad functions of the eSafety Commissioner.
* The eSafety Commissioner current administers a number of complaints and take down services which can be applied to social media platforms:
  + a complaints scheme for cyberbullying targeted at an Australian child; including removal of cyberbullying material;
  + an image-based abuse portal to facilitate the removal of intimate images shared without consent, i.e. revenge porn. Legislation currently before the Parliament will empower the eSafety Commissioner with civil penalties to take action against perpetrators, social media services and content hosts; and
  + Administration of the Online Content Scheme (Schedules 5 & 7 of *Broadcasting Services Act 1992*) for prohibited online material.

These roles are explained in more detail below.

*Cyberbullying Complaints Scheme*

* The cyberbullying complaints scheme is designed to quickly remove cyberbullying material that is harmful to a child from large social media sites. It is a world first complaints system where children, parents and teachers can lodge a complaint and receive timely advice and assistance.
* In order to lodge a complaint with the eSafety Commissioner, a complaint must first be made to the relevant social media service under its complaints scheme. If the service does not remove the material within 48 hours, a complaint can then be made to the eSafety Commissioner. Each complaint received by the Commissioner is assessed on a case-by-case basis.
* Under the legislation, the eSafety Commissioner has two sets of powers to deal with a cyberbullying complaint:
* First, the eSafety Commissioner is able to issue notices to large social media services to remove cyberbullying material targeted at an Australian child from the service.
* Second, the eSafety Commissioner is able to give a notice to a person who posts cyberbullying material targeted at an Australian child on either a social media service or a ‘relevant electronic service’ (e.g. email, text message).
* The scheme involves a two-tiered system, backed by legislation, to apply to social media services accessible to Australian children. Social media services participating under tier 1 participate on a cooperative basis and are not be subject to legally binding notices or penalties. These social media services generally have robust, well-established mechanisms for handling complaints and the scheme is designed to interwork with these existing processes. Those declared to be tier 2 social media services are subject to legally binding removal notices and face civil penalties for non-compliance.
* The eSafety Commissioner works collaboratively with key social media services to rapidly remove cyberbullying material. While the eSafety Commissioner does not have the authority to compel sites and services hosted overseas (and not social media partners with the Commissioner under the two-tiered scheme) to remove content, many of these sites and services remove content at the eSafety Commissioner’s request on a voluntary basis.
* The eSafety Commissioner continues to engage with smaller app developers individually in a bid to get more services formally into the two-tiered scheme. The eSafety Commissioner believes that more could be achieved if more requirements are placed on the gaming and app stores platforms to also comply with the Basic Online Safety Requirements established under the Online Safety Act.

*Non-Consensual Sharing of Intimate Images*

* The Australian Government considers the non-consensual sharing of intimate images, or ‘revenge pornography’, a grave violation of a person’s freedom.
* The Enhancing Online Safety (Non-consensual sharing of intimate images) Bill 2018 is currently before the Australian Parliament. The Bill makes it an offence to post, or threaten to post, an intimate image on a social media site, via email or SMS, or on a website without consent. Civil remedies can be applied to both the perpetrator and content host, and to social media and content providers who fail to comply with a request to remove offending material.
* The eSafety Commissioner will be empowered with enforcement capabilities, including the ability to take fast and effective action to have images removed and to limit further sharing of images, which is the primary concern of victims.
* The civil penalty regime will complement the national portal launched by the eSafety Commissioner on 16 October 2017. The portal allows persons to report instances of non‑consensual sharing of intimate images. The portal is a world first government-led initiative and provides immediate and tangible support to victims of image‑based abuse.

*Online Content Scheme*

* The Online Content Scheme, set out in Schedules 5 and 7 of the *Broadcasting Services Act 1992*[[3]](#footnote-4), regulates prohibited and potential prohibited online content in Australia based on the National Classification Scheme. The scheme is complaints-based and applies to content accessed through the Internet, mobile phones and convergent devices, as well as subscription-based internet portals, chat rooms, live audio-visual streaming, and link services.
* The scheme aims to address community concerns about offensive and illegal content online, and help protect children from exposure to inappropriate material.

The scheme empowers the eSafety Commissioner to investigate complaints and take action if the content is “prohibited” or “potentially prohibited”. Prohibited content includes content that has been classified by the National Classification Board as:

* + *Refused Classification* – includes child sexual abuse material, material that advocates the doing of a terrorist act, detailed instruction or promotion in crime or violence, instruction in paedophilic activity, gratuitous, exploitative and offensive depictions of violence or sexual violence
  + *X18+* - content that contains explicit sexual activity between adults
  + *R18+, unless it is subject to a restricted access system* – content that is of high impact and includes realistically simulated sex, violence, drug use or nudity
  + *MA15+ and is provided on a commercial basis, unless it is subject to a restricted access system* – content is strong impact

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

* These prohibitions are backed by strong sanctions for non-compliance including criminal penalties for serious offences.
* Where prohibited content is hosted in Australia, the eSafety Commissioner can direct the content service provider to remove the content from their service. Where prohibited content is not hosted in Australia, the eSafety Commissioner will notify approved filter suppliers about the content, so that access to the content using such filters is blocked.
* Regardless of where content is hosted, if the eSafety Commissioner considers the content to be of a sufficiently serious nature, it must notify an Australian police force.

**Terrorist or violent extremist content**

* The Australian Government believes that the maintenance of security online and the protection of freedom online reinforce each other. A secure cyberspace provides trust and confidence for Australians. This underpins freedom of expression and reinforces safe and vibrant communities. The Australian Government works with the private sector to promote corporate responsibility for a safe, open and secure internet.
* The Australian Government maintains cooperative relationships with social media companies to encourage industry-led action to curtail the spread of terrorist and violent extremist content on their platforms.
* The Government refers content that it has identified in open source forums to social media platforms for review and voluntary removal where it breaches the company’s terms of service. The Government uses the social media platforms’ publicly available mechanisms for flagging content. The focus of this cooperative arrangement is referring for review any content that:
  + provides instructions to commit an offence associated with terrorism;
  + is extremely graphic in nature; or
  + expressly promotes or advocates violence against individuals or organisations.
* The National Cyber Security Advisor also engages with industry to further promote corporate responsibility for safe, secure and free internet.

**Other Commonwealth, State and Territory Laws**

* Australia has existing laws that protect fundamental human rights which can be applied to online behaviour or content.

*Criminal Code Act 1995*

* Under the Commonwealth *Criminal Code Act 1995* (Criminal Code), it is a crime to use the internet or phone in a *menacing, harassing or offensive* way[[4]](#footnote-5). It is also an offence to use the internet or phone to threaten to kill or cause serious harm to another person[[5]](#footnote-6). Maximum penalties for these offences range from three to ten years imprisonment.
* Section 474.25 of the Criminal Code requires an internet service provider or content host to refer details of child abuse material to the Australian Federal Police, where it becomes aware that the service can be used to access that material. The maximum penalty for this offence is 100 units.

This provision does not require internet service providers and content hosts to monitor their services for child abuse material, but rather ensures that material is referred for law enforcement consideration when the service provider becomes aware of the existence of the material.

* Each state and territory has anti-stalking and threatening behaviour laws which may apply to online behaviour such as cyberbullying. States and territories also have their own defamation laws which may apply to online content.

*Anti-discrimination laws*

* Issues relating to online content can be the basis for complaints to the Australian Human Rights Commission under federal anti-discrimination law[[6]](#footnote-7) (for example, online content that is alleged to constitute sexual harassment or racial vilification). Parallel legislation exists in all states and territories.

*Suicide Related Material Offences 2005*

* In 2005, the Australian Parliament passed the *Criminal Code Amendment* (*Suicide Related Material Offences) Act 2005[[7]](#footnote-8)*, which makes it illegal to use a carriage service to access, transmit or otherwise make available suicide related material, and possession, production, supplying or obtaining suicide related material for use through a carriage service

**INTERPOL and Section 313 Telecommunications Act 1997 (Cth)**

* Section 313[[8]](#footnote-9) of the *Telecommunications Act 1997* (Cth) provides Australian government agencies, including state government agencies, with the ability to obtain assistance from the telecommunications industry when upholding Australian laws.
* The Australian Federal Police (AFP) has responsibility for website blocking requests under section 313 of the *Telecommunications Act 1997*.
* Subsection 313(1) of the *Telecommunications Act 1997* (Cth) imposes obligations on internet service providers to do their best to prevent telecommunications networks from being used to commit Commonwealth offences.
* Subsection 313(3) of the *Telecommunications Act 1997* (Cth) imposes obligations on internet service providers to provide officers and authorities of the Commonwealth and of the States and Territories to provide such help as is reasonably necessary for the following purposes:
  + enforcing the criminal law and laws imposing pecuniary penalties;
  + the enforcement of the criminal laws in force in a foreign country;
  + protecting the public revenue; or
  + safeguarding national security.
* The AFP uses section 313(3) requests to disrupt illegal online activity where other mechanisms have been or are likely to be unsuccessful.
* Through the Access Limitation Scheme, the AFP predominantly uses section 313(3) requests to block access to INTERPOL’s ‘Worst of List’ of child exploitation websites. When an Australian user attempts to access a website contained on the Worst of List, they are redirected to an INTERPOL ‘stop page’, blocking access to information containing child abuse material. The AFP provides the list to Australian internet service providers, and relies on them to block the identified websites in Australia.
* Websites included on the INTERPOL ‘Worst of List’ depict some of the most severe child sexual exploitation material.
* The AFP believes blocking of this known criminal content is a proactive, disruption strategy which is a positive step in helping to protect children from sexual exploitation and abuse.

**Referrals to AFP and eSafety Commissioner – content on social media sites**

* There are distinct differences between referrals to the AFP and referrals to the eSafety Commissioner, these being:
  + AFP referral: information that could lead to the criminal investigation of an Australian child sex offender, or the identification of a child or other person, and there is an Australian link to a child exploitation matter; and
  + eSafety referral: information that identifies inappropriate content, including child abuse material, hosted inside Australia where a takedown of the host will not compromise any ongoing AFP investigation.
* The AFP refers matters to the eSafety Commissioner on a regular basis (approx. 2 per month). These referrals may involve reports from members of the public who believe a web link contains offensive material including possibly child exploitation material (CEM). The AFP confirms if CEM is on the site and, if so, the AFP refers the matter to eSafety.
* The AFP encourages those wishing to make reports regarding cyberbullying or image based abuse to report the cyberbullying or abuse to the site on which the material is hosted in the first instance. If the material is not removed following complaint, the AFP encourages them to report this eSafety Commissioner to facilitate the removal. These details are captured in the updated 2018 ThinkUKnow presentations which are being delivered to communities across the country.

**Human rights scrutiny – Statements of Compatibility**

All government and non-government Bills and disallowable legislative instruments introduced into the Federal Parliament must be accompanied by a Statement of Compatibility. A Statement of Compatibility must contain an assessment of the Bill or legislative instrument's compatibility with the rights and freedoms recognised in the seven core international human rights treaties which Australia has ratified, including the Covenant. This process encourages early and ongoing consideration of human rights in policy and legislative development.

The Attorney-General’s Department and the Parliamentary Joint Committee on Human Rights issue guidance documents to assist public servants to assess the human rights compatibility of policy and legislation and to draft Statements of Compatibility. The Human Rights Unit within the Attorney-General’s Department consult on draft Statements of Compatibility and provide additional assistance to public servants as requested.

**Parliamentary Joint Committee on Human Rights (PJCHR)**

The Parliamentary Joint Committee on Human Rights (PJCHR) examines and reports on the human rights compatibility of all bills and legislative instruments that come before the Parliament. It plays an important role in promoting dialogue about and recognition of human rights in the Parliament and in the broader community. Its work is considered in developing and refining legislation.

The PJCHR generally meets when both Houses of Parliament are sitting, and has a regular reporting cycle around these meetings. Reports are tabled after each meeting, and deal with the bills and instruments of delegated legislation introduced or tabled in the preceding period.

Where a bill or instrument limits a human right, the Parliamentary Joint Committee on Human Rights requires that the Statement of Compatibility provide a detailed and evidence-based assessment of the measures against the limitation criteria. If the Committee considers that a Statement of Compatibility does not include a reasoned and evidence-based assessment, the Committee will write to the relevant Minister seeking further information.

The PJCHR seeks to conclude and report on its examination of bills while they are still before the Parliament, so that its findings may inform legislative deliberations. However, this is dependent on the legislative program of the government of the day and the timeliness of ministers' responses to the PJCHR’s inquiries.

Where a bill is passed before the PJCHR has been able to conclude its examination, the PJCHR nevertheless completes its examination of the legislation and reports its findings to the Parliament. Its work may then influence refinement of the legislation.

The PJCHR may also consider the human rights compatibility of existing legislation and has self-initiated inquiries into human rights issues in certain circumstances. The Attorney-General may also refer any matter relating to human rights to the PJCHR for inquiry and report.

*Parliamentary committee inquiries into issues of human rights concerns*

Parliamentary human rights scrutiny is not limited to the Parliamentary Joint Committee on Human Rights. There are a number of parliamentary committees in the Australian Parliament which are able to conduct inquiries into issues raising human rights concerns.

This includes for example, the Senate Committee on Community Affairs, the Senate Standing Committee on Legal and Constitutional Affairs, the Parliamentary Joint Committee on Intelligence and Security and the Parliamentary Joint Committee on Law Enforcement.

1. *Enhancing Online Safety for Children Act* *2015* (Cth) <https://www.legislation.gov.au/Details/C2017C00187> [↑](#footnote-ref-2)
2. *Enhancing Online Safety Act 2015* (Cth) s 15.<https://www.legislation.gov.au/Details/C2017C00187> [↑](#footnote-ref-3)
3. *Broadcasting Services Act 1992* (Cth) Schs 5,7 <https://www.legislation.gov.au/Details/C2017C00346/Html/Volume_2> [↑](#footnote-ref-4)
4. *Criminal Code Act* *1995* (Cth) s474.17. [↑](#footnote-ref-5)
5. Ibid. [↑](#footnote-ref-6)
6. *Racial Discrimination Act 1975* (Cth). [www.comlaw.gov.au/Details/C2014C00014](http://www.comlaw.gov.au/Details/C2014C00014)

   *Sex Discrimination Act 1984* (Cth). [www.comlaw.gov.au/Details/C2014C00002](http://www.comlaw.gov.au/Details/C2014C00002)

   *Age Discrimination Act 2004*(Cth). www.comlaw.gov.au/Details/C2014C00435 [↑](#footnote-ref-7)
7. *Criminal Code Amendment (Suicide Related Material Offences) Act 2005* (Cth). [www.comlaw.gov.au/Details/C2005A00092](http://www.comlaw.gov.au/Details/C2005A00092) [↑](#footnote-ref-8)
8. *Telecommunications Act 1997* s313 (Cth). [www.comlaw.gov.au/Details/C2012C00584](http://www.comlaw.gov.au/Details/C2012C00584) [↑](#footnote-ref-9)