Statutory Review of the Online Safety Act 2021

OVERVIEW

The global information environment is part of modern Australian political, economic and social life, bringing with it new kinds of connectivity and opportunity. At the same time, it is a vector for serious threats – in particular the impact of disinformation.

Coordinated disinformation campaigns have grown in intensity, affecting many areas of Australian public life. Of particular concern is the growth of disinformation groups in Australia. This includes threats to public health via the spread of disinformation around COVID-19 vaccination; the targeting of Australian public servants, as evidenced by unprecedented threats of violence against Australian Electoral Commission; well-funded disinformation campaigns against action to mitigate carbon emissions; and the mainstreaming of disinformation as tool of political campaigning.

Compounding these vulnerabilities is the existing low level of public literacy on threats in the information environment and a lack of easy-to-use information and services to empower individuals and groups to protect themselves from harm. There is a serious threat that foreign countries use information warfare techniques to erode Australia's multicultural identity and social cohesion and to promote political and economic elites that are friendly to their economic and political objectives.

Acknowledging that "Cyber is no longer a technical topic but a whole-of-nation effort", the 2023-2030 Australian Cyber Security Strategy commits to "deploy all arms of statecraft to deter and respond to malicious cyber actors."

This submission offers recommendations for how Australia can use all tools of statecraft to shape an information space more conducive to Australia's interests. It draws on consultations with some of Australia's foremost experts on information and communications practices compiled by the Asia-Pacific Development, Diplomacy & Defence Dialogue (AP4D) in its recently-released report.[1]

The recommendations in this submission primarily relate to part three of the issues paper:

> *Protecting those who have experienced or encountered online harms*

In particular, question 16:

> *What more could be done to promote the safety of Australians online, including through research, educational resources and awareness raising?*

[1] See Asia-Pacific Development, Diplomacy & Defence Dialogue, *What does it look like for Australia to all tools of statecraft in the information environment* (Canberra 2023): https://asiapacific4d.com/idea/information-environment/

RECOMMENDATIONS

1. A national body for the information environment

There is the danger of a siloed way of thinking about threats in the information environment, such as cybersecurity, disinformation, social cohesion, foreign interference, data, privacy and criminal exploitation. Agencies do not naturally share information/analysis in a truly integrated way and the best current practice is often to coordinate through interdepartmental taskforces or similar mechanisms. These are usually built around single issues and are non-enduring. Legislation and separation of powers often present barriers to whole-of-government action.

Australia should create a national body that identifies and pre-empts emerging problems in the information environment and then marshals resources and expertise to find solutions. This body would draw together and coordinate work being done in individual agencies across government and include mechanisms to engage in dialogue with, and draw on the expertise of, non-government actors such as industry, civil society, non-governmental organisations and academics working in the space.

Such a body would help government create a strong, enforceable regulatory framework that sets a standard of conduct, as well as legal parameters for foreign technology companies operating in Australia. It should function as a vehicle that promotes constant dialogue between government, industry and the Australian public.

It may also be useful to create teams in government departments with a single dissemination point that are responsible for calling out coordinated disinformation that targets Australia as soon as it appears. This would demonstrate to the public and disinformation networks that the government is aware and responding. This could be especially valuable in a time of national or regional crisis. One model could be the Department of Foreign Affairs and Trade's Smartraveller program.

2. Support Australian diasporas targeted by disinformation and harassment campaigns

As an adjunct to a national, strategically focused body, Australian intelligence and security organisations should work more closely with other government bodies to strengthen the capacity to provide tangible and rapid support to Australian citizens targeted by malicious foreign actors. As a first step, the government should undertake a multilingual campaign to raise awareness of the national security hotline among members of the public who may not be aware of it.

Interference in Australia's Iranian, Chinese, Russian, Ukrainian, Rwandan and Sudanese communities has been well-documented and is likely to keep increasing. This targeting can include repeated and persistent online threats of physical violence to individuals and their families, false accusations of criminal activity, persistent dehumanising language and the hacking of citizens' computers.

In addition to increased information sharing and collaboration between security and intelligence organisations and other government agencies, a rapid response capability could be achieved by further expanding the remit of, and a concomitant increase in resourcing for, the eSafety Commissioner to support diaspora groups being targeted. As the most public-facing Australian body for safety from online crime and exploitation, embedding such a mandate within the eSafety Commissioner is an option that is less likely to trigger political sensitivities.

3. Public literacy and information campaign

Australia should commit more resources to protecting citizens from harms in the information environment – such as disinformation, foreign interference, identity theft, surveillance and exploitation – through long-term well-funded and ongoing public literacy campaigns that are designed to reach diverse audiences.

These campaigns should empower citizens to discern the accuracy of the information they see online, to encourage the promotion of accurate information in information systems, and to protect citizens from exploitation through information systems, including through appropriate reporting and assistance mechanisms.

A key feature of this would be a comprehensive digital media literacy campaign that clearly articulates:

- values of press freedom, media ethics, privacy and freedom of speech
- what constitutes hate speech, on-line bullying and trolling, disinformation and propaganda
- the critical thinking skills needed to be resilient in the face of cognitive manipulation and exploitation
- how to navigate the internet as synthetic, manipulated images and text created by generative AI become widespread

The program should be well-funded, long-term and take place from primary education level onwards. The content should be fun and engaging, with face-to-face learning and collective problem solving emphasised. This would need to include support for educators and teachers to help them combat disinformation in the classroom.

In addition to broad based public awareness campaigns, digital media literary needs to be included in education curriculums from early childhood onwards in order to help children and young adults build resilience against the many harms targeted at them in the information environment.