Executive Manager, Investigations
Office of the eSafety Commissioner
PO Box Q500
Queen Victoria Building
NSW 1230
submissions@esafety.gov.au

**Submission: Draft RAS Declaration**

This submission responds to the Commissioner's call for public comment on the draft Online Safety (Restricted Access Systems) Declaration 2021 under subsection 108(1) of the *Online Safety Act 2021* (Cth).

Following pages offer contextualisation before addressing specific concerns regarding the draft Declaration.

**Summary**

Overall the RAS Declaration constructs a digital Potemkin Village, a regime that may be politically convenient as we head towards an election but which ignores the very substantial body of Australian/overseas research regarding online safety and is very unlikely to be effective.

Its ineffectiveness is of particular concern given indications that the regime will exacerbate harms that are inadequately addressed under Australian law, in particular privacy.

Extension of the Commissioner's powers and establishment of a structurally flawed RAS regime is of particular concern given the Commissioner's disclosure that she has never exercised her powers under the current RAS.

**Basis**

The submission reflects scholarly research and teaching over the past fifteen years regarding online content regulation, harms and mechanisms for strengthening the capacity of vulnerable people such as minors. It draws on teaching regarding cybercrime, digital network management and privacy. It also draws on forthcoming monographs regarding identity crime (including impersonation and identity verification in online environments) and personhood, alongside invited submissions to a range of Commonwealth/state parliamentary committees and law reform commissions over the past twenty years.

The submission does not represent what would be reasonably construed as a conflict of interest.

Dr Bruce Baer Arnold
Associate Professor
Canberra Law School
University of Canberra

14 November 2021

# draft Online Safety (Restricted Access Systems) Declaration 2021

## Context

Public and private efforts to minimise harms to vulnerable people, in particular young Australians, are commendable. Australia (along with other liberal democratic states) does not have an absolute freedom of expression. Australian courts, alongside human rights advocates, have properly endorsed constraints that range from bans on the advertising of tobacco products[1] through to prohibitions on hatespeech,[2] respect for autonomy through 'safe zones' around health facilities[3] and rules regarding activity in public spaces.[4]

It is important to recognise, however, that Australia is a pluralist society where people legitimately hold differing views regarding expression and morality. Australia's history of content regulation regarding print, film and broadcast illustrates that action by governments at the Commonwealth and state/territory level has often been –

- highly politicised (notably to satisfy stakeholders whose views were not shared by most of the community or to gain a political advantage prior to an election),
- inappropriately administered (for example media-driven opportunistic 'spectacles' such as police raids seizing content that was not illegal),
- at the expense of substantive measures such as education that strengthen the capability of those people who are deemed to be vulnerable,
- an expression of moral panics regarding comics, 'video nasties', fertility advice, long hair, rock music or labour unrest, and
- targeted at groups such as gay men, women seeking control over their own bodies, the economically disadvantaged and Indigenous people in ways that denied dignity and harmed those people.

That history means the eSafety Commissioner, whose authority is discussed below, and the Government should be very wary about repeating the past in search of institutional benefit and political advantage. Fast-tracking the RAS without regard for the Classification Review places the cart before the horse, indeed tacitly dispensing with both the horse and a robust community consideration of content regulation objectives and capabilities.

It is administratively convenient to market the RAS as an effective and necessary mechanism for protecting 'young people' from harm and responding to #metoo advocacy after a succession of incidents in which the Government failed to walk the talk about respecting women. It is however fundamentally important not to objectify everyone under the age of 18 (an arbitrary date) as having the same characteristics. The 'youth' cohort, just like the Australian community, is very broad, with major differences on the basis of formal education, guidance by peers, personal experience, supervision by a parent/guardian, health, gender, economic circumstances, intelligence and robustness. Australian law properly recognises differences between a five year old and an eighteen year old, challenges with psychiatric/psychological difference, recognition of autonomy through Gillick Competence,

---

[1] *JT International SA v Commonwealth of Australia* [2012] HCA 43.
[2] *Man Horan Monis v The Queen & Anor and Amirah Droudis v The Queen & Anor* [2013] HCA 4.
[3] *Kathleen Clubb v Alyce Edwards and Anor; John Graham Preston v Elizabeth Avery and Anor* [2019] HCA 11.
[4] *Attorney-General for the State of South Australia v Corporation of the City of Adelaide & Ors* [2013] HCA 3; and *O'Flaherty v City of Sydney Council* [2013] FCA 344.

the lawfulness of consensual sexual activity by young adults and the legitimacy of sexual difference.

It is also fundamentally important not to institute a regulatory scheme that is ineffective (notably because it will be readily and widely subverted by those people it supposedly protects), that is inconsistent with other regulatory initiatives and embodies inadequate governance. As with past versions of the legislation, there is a danger that promotion of the RAS regime will mislead some people that the regime is effective and parents/guardians accordingly not need to be vigilant in guiding and protecting minors.

A succession of authoritative independent reports have identified ongoing erosion of community distrust of –

- politicians (perceived as lacking integrity and strongly resistant to anti-corruption initiatives) and
- an increasingly politicised public service that has both been captured by particular stakeholders and is subject to inadequate governance (including transparency about its operation, reliance on non-substantive 'consultation theatre' in policy implementation such as the current RAS, and supervision by regulators that lack capability).

It is therefore particularly disquieting that the Government is fast-tracking the RAS Declaration prior to finalisation of the Classification Review, proposed changes to the *Privacy Act 1988* (Cth), the Government's emphasis on cyber security and initiatives such as the Digital Trusted Identity Framework. That haste and incoherence serves to erode the legitimacy of the Commissioner's operation in the eyes of industry and the broader community.

**Subversion**

Industry experience and scholarly research in Australia and overseas have demonstrated that age-based digital identity mechanisms are unlikely to be effective. That ineffectiveness is not new and it is accordingly disquieting that the RAS appears to be predicated on exclusion of young people from what is deemed to be improper content on the basis of –

- an online or print statement of a potential user's age, or
- 'verification' of such a statement by reference to credit card details (name, number, code).

Many young people are comfortable providing a false date of birth and/or false name. In part that is an assertion of their autonomy, in other words the sort of thing – rule breaking and rule testing – that teenagers and their younger peers do in the course of growing up as resilient people rather than incapacitated 'cotton-wool kids'. In part it is a reasonable response to community recognition that 'surveillance capitalism' (including the commercial rationales of digital platforms such as Facebook and Google that were explored by the Australian Competition & Consumer Commission's *Digital Platforms* report) is based on the systemic collection and exploitation of identity data without real regard for security.

Over the past two decades governments have raised consciousness about 'identity theft', on occasion conflating different types of identity offences and leveraging problematical statistics to introduce identity schemes that both erode privacy and exacerbate offences. Hyperbole about the incidence and severity of finance-driven identity offences tends to obscure the reality that many misuses of an individual's credit card, debit card, PayPal account or traditional cheque account involve people known to that individual, including offspring, partners and siblings, rather than a cyber wizard located in Vladivostok or the "Nigerian Prince' and 'Saddam Hussein Cousin' located in Amsterdam.

Comprehensive verification of age on the basis of an asserted name + birthdate plus credit card details is wide open to subversion. Few parents keep their cards in a vault; many young people have overt or covert access to details that will allow them to successfully subvert the age-based regime. Subversion of the regime by a teenager is just a laptop or wallet away.

One response to that subversion might be for the Government, in cooperation with the states and territories, to engage in a substantive community education campaign regarding –

- the appropriateness of parents/guardians providing nuanced guidance to and supervision of young people in their care – nuanced to the differing capabilities and emerging autonomy of people who are under 18
- the realities of identity theft rather than scare campaigns

One reason for that nuance – and for disquiet about the regime's bundling of everyone under 18 as having the same vulnerability that requires the same disregard of dignity – is that both young people and law recognise some ages as having more capability than others. I have referred above to Gillick Competence, something most appropriately evaluated on an instance by instance basis. In cautioning about objectification – treating a sixteen year old as having the skills, experience and fragility of a six year old – I note that although the RAS regime appears to be intended to prevent the teenager from independently accessing adult content the same person is lawfully able to engage in consensual activity sexual activity (including activity that causes Israel Folau and other polemicists to shudder) prior to the age of 18.

**Privacy**

The fast-tracking of the RAS for political advantage pre-empts both the Classification Review and reviews of the national privacy regime. That is of concern because it risks, if not guarantees, regulatory incoherence that imposes an inappropriate burden on industry and further confuses individuals.[5] It is also of concern because the age-regime noted above and alternate regimes (such as extension of the deeply flawed Trusted Digital Identity Framework or biometric verification specific to a particular digital platform) foster privacy harms without providing commensurate remedies.

The Explanatory Statement regarding the RAS states –

> Age confirmation methods **should** be privacy-preserving. They should limit the scope of information collected by the system to ensure the only attribute being tested is the age of the applicant. For the avoidance of doubt, age confirmation does **not** involve identity verification.

Given the weakness of the existing privacy regime (including the absence of a cause of action for serious invasion of privacy, weak oversight by an under-resourced Office of the Australian Information Commissioner, and inadequate penalties) it is disquieting that the reference is to "should" rather than "must" be privacy preserving. "Should" signals to entities under the Act that privacy, just like probity among politicians, is not taken very seriously and that disregard of privacy will be permitted.

The characterisation exacerbates rather than avoids confusion by stating that age verification does not involve identity verification. Biometric schemes used to verify a claim of age will necessarily involve personal information; they will involve a particular identity verification. Reliance on credit card or similar financial identifiers will also involve identity verification.

---

[5] The latest Privacy Bill enshrines a separate age verification regime for "social media", defined differently to the Online Safety Act.

The characterisation is thus problematical: a scheme that relies on age, is meant to be effective rather than a regime of pasteboard & tinsel, but does not involve identity?

The proposed RAS involves a high degree of subjectivity, with the Commissioner (having exceptional autonomy weakly bounded by potential referral of decisions to the Ombudsman and Administrative Appeals Tribunal) deciding what is "reasonable" for individual entities covered by the Act. Greater attention to privacy is fundamental given the history of large-scale data breaches involving sites with age-restricted content. The Ashley Madison data breach is not isolated. During the course of writing this submission the StripChat breach for example involved exposure of the personal data of between 65 million and 200 million people.

If the Commissioner **is** going to require 'age verification' that in fact involves identity verification it is imperative that the regime requires substantive privacy protection. People who lawfully access age-restricted content should not be imperilled because the Commissioner considers privacy protection should – but need not be – taken into consideration. People whose identifiers have been misused by family members or others seeking access (irrespective of whether that misappropriation is detected and access refused) should also not be imperilled.

Transparency is one basis of good government. Three starting points for a more trusted regime are –

- publication by the Commissioner of detailed guidance about what is "reasonable" for large and small entities implementing the RAS
- a public commitment by the Commissioner to requiring privacy protection as part of what is "reasonable"
- a community education program that acknowledges criticisms of past Commissioner safety awareness campaigns, ie moves beyond mousemats and media releases.