Restricted Access System Declaration Online Safety Act 2021

Discussion Paper

Submission by the Australian Communications Consumer Action Network to the eSafety Commissioner

17 September 2021

Australian Communications Consumer Action Network (ACCAN)
Australia's peak telecommunications consumer organisation

PO Box A1158, Sydney South NSW 1235
Tel: (02) 9288 4000 | Contact us through the National Relay Service
www.accan.org.au | info@accan.org.au | twitter: @ACCAN_AU

About ACCAN

The Australian Communications Consumer Action Network (ACCAN) is the peak body that represents all consumers on communications issues including telecommunications, broadband and emerging new services. ACCAN provides a strong unified voice to industry and government as consumers work towards communications services that are trusted, inclusive and available for all.

Consumers need ACCAN to promote better consumer protection outcomes ensuring speedy responses to complaints and issues. ACCAN aims to empower consumers so that they are well informed and can make good choices about products and services. As a peak body, ACCAN will represent the views of its broad and diverse membership base to policy makers, government and industry to get better outcomes for all communications consumers.

ACCAN

PO Box A1158,
Sydney South NSW, 1235
Email: info@accan.org.au
Phone: (02) 9288 4000
Contact us through the National Relay Service

17 September 2021

Office of the eSafety Commissioner

PO Box Q500

Queen Victoria Building NSW 1230

submissions@esafety.gov.au

ACCAN thanks the eSafety Commissioner for the opportunity to contribute to its RAS Declaration Online Safety Act 2021 Discussion Paper.

ACCAN welcomed the introduction of the Online Safety Act 2021 which is intended to create a modern, fit for purpose regulatory framework that builds on the strengths of the existing legislative scheme for online safety. The inclusion of serious child cyberbullying and seriously harmful adult cyber abuse in the Act, are a positive extension of the existing regime designed to tackle image-based abuse.

In many areas of regulation of the internet and other emerging technologies, the difficulties of successfully controlling online content has meant that responsibility has been shifted to consumers to protect themselves. This is also the case with restriction of content available to children and minors, where historically at least part of the responsibility to protect minors from harmful online content has been held by parents and guardians.

The new options for enforcement available to the eSafety Commissioner, including removal and remedial notices, are a positive new development in online regulation. The scope and ubiquity of online content, and the number of devices that can be used to access the content, has expanded exponentially since 2014. This change has made it increasingly unrealistic for parents and guardians to monitor all of the online content that their children consume at all times.

Providing consumer education about 'cyber hygiene' to parents, guardians and children continues to be a vital component in the restriction of children's access to inappropriate content. However, ACCAN submits that there is a need for stronger and more effective regulation to protect children from exposure to explicit content including material rated MA15+ and R18+.

The eSafety Commissioner's strengthened enforcement powers under this new Act, supported by a new Restricted Access System Declaration (RAS), will relieve the pressure on parents and guardians to take full responsibility for restricting their children's access to harmful content online.

ACCAN will address the individual questions raised in the Discussion Paper below.

Restricted Access System Effectiveness and Impacts

1. ***Under the Online Safety Act 2021, the RAS will only apply to Restricted Material that is provided from Australia on a social media service, relevant electronic service or designated internet service, or that is hosted in Australia. What elements should be part of an effective system to limit access to that kind of material?***

An underlying weakness of the RAS is that it only applies to restricted material that is provided from Australia or that is hosted in Australia, and VPN services allow consumers to access material that is provided or hosted outside Australia. Content providers outside Australia may be unlikely to comply with Australian obligations to restrict access to adult content. Any age verification system that is introduced will not, therefore, limit children's access to all potentially harmful content. Despite this, ACCAN welcomes the revised Restricted Access System Declaration as a method of imposing access restrictions on the platforms from which large proportions of the Australian public access media content.[1]

Although it was never implemented, the UK's proposed age verification system under the *Digital Economy Act* has some elements that could be drawn on in developing an Australian age verification system which is both effective and secure.

First, the British Board of Film Classification (BBFC) was designated as the age-verification regulator under the scheme, and it was responsible for providing guidance and assessing content providers for compliance with the Act. The criteria that content providers had to meet included:

- an effective control mechanism at the point of registration or access to pornographic content by the end-user which verifies that the user is aged 18 or over at the point of registration or access;
- use of age-verification data that cannot be reasonably known by another person, without theft or fraudulent use of data or identification documents nor readily obtained or predicted by another person;
- a requirement that either a user age-verify each visit or access is restricted by controls, manual or electronic, such as, but not limited to, password or personal identification numbers. A consumer must be logged out by default unless they positively opt-in for their log-in information to be remembered; and
- the inclusion of measures which authenticate age-verification data and measures which are effective at preventing use by non-human operators including algorithms.[2]

Australian consumers would benefit from an independent body performing the same function, reviewing age verification practices and RAS compliance on all social media services, designated internet services and relevant electronic services – email, messaging services, chat services, online

[1] https://www.alrc.gov.au/publication/classification-content-regulation-and-convergent-media-alrc-report-118/10-restricting-access-to-adult-content/restricting-access-to-adult-content/

[2] https://www.aph.gov.au/Parliamentary_Business/Committees/House/Social_Policy_and_Legal_Affairs/Onlineageverification/Report/section?id=committees%2Freportrep%2F024436%2F72614

gaming - that are providing access to material from Australia, as well as Australian hosting service providers.

Second, in addition to providing guidance to age-verification providers, the BBFC established a voluntary, non-statutory certification scheme—the Age Verification Certificate (AVC) – developed in collaboration with cyber security and risk mitigation experts and industry and supported by government. Under the AVC, age-verification providers could choose to be independently audited by a third party to measure their compliance with strict privacy and data security requirements, and then certified by the BBFC. Compliant providers could then display a certification symbol.[3]

This approach could also be adopted in Australia. Third party auditing of compliance with the RAS, and transparency in compliance indicated by a symbol, would reassure Australian consumers and reinforce their confidence in using an age verification system. It would also hold age verification providers to account and give them an opportunity to advertise their high data protection standards. ACCAN would prefer such a scheme to be compulsory rather than voluntary, although we acknowledge that in the UK many of the major age verification providers did seek certification voluntarily.

Third, ACCAN would endorse the introduction of an Age Checking Code of Practice in Australia, similar to the PAS 1296[4] published by the British Standards Institute in March 2018. A Code of Practice would assist age-verification providers to comply with legal requirements under the RAS using similar 'vectors of trusted' in the PAS 1296 which were:

- identity proofing (how strongly the set of identity attributes has been verified and vetted);
- primary credential usage (how strongly the primary credential can be verified);
- primary credential management (the use and strength of policies, practices, and security controls used in managing the credential); and
- assertion presentation (how well the given digital identity can be communicated across the network without information leaking to unintended parties, and whether the given digital identity was actually asserted by the given identity provider).[5]

2. Has industry experienced any difficulty complying with the Restricted Access System Declaration 2014?

N/A

3. Has the Restricted Access System Declaration 2014 allowed industry the flexibility to develop access-control systems appropriate to their business models?

N/A

---

[3] British Board of Film Classification, Submission to the Australian Government's Inquiry into Age Verification for Online Wagering and Online Pornography, October 2019, p. 11

[4] https://www.dpalliance.org.uk/pas-1296-online-age-checking-code-of-practice/

[5] TrustElevate, Submission to the Australian Government's *Inquiry into Age Verification for Online Wagering and Online Pornography*, October 2019, pp. 2-3.

See also: Dr Rachel O'Connell, Co-founder, TrustElevate, *Committee Hansard*, Canberra, 5 December 2019, pp. 12-13

4. ***What is the nature of the impact that has been experienced by (b) the Australian public as a result of the Restricted Access System Declaration 2014? Have there been any indirect effects (for example, costs being passed on to customers or suppliers)? Please provide examples.***

ACCAN is unaware of any negative impacts on the Australian public or customers as a result of the Restricted Access System Declaration 2014. However, submissions to the *Inquiry into Age verification for Online Wagering and Online Pornography* suggested that minimal burden was imposed on businesses and consumers in adhering to age verification practices.

In fact, the BBFC submitted that age verification was a 'simple and affordable option' for online platforms. Similarly, TrustElevate submitted that the commercial models that underpin an identity ecosystem allow businesses to perform age verification for free or at low cost.[6]

Nor is the impact on consumers of online age verification burdensome, as proof of age is all that is required. However, ACCAN submits that it is important to make a range of age verification options available to consumers to provide maximised choice and accessibility and minimise security risks.

Age restriction methods

5. ***What factors should be considered when assessing the effectiveness and impacts of systems, methods and approaches to limiting access or exposure to age-inappropriate material?***

There is a need for the Restricted Access System Declaration to be fine-tuned so that it is not a blunt instrument that may have unintended consequences of blocking or taking down legitimate content, as in the case of Facebook blocking free access to news content in 2020.[7]

For example, there are aspects of some material which might be considered educational when viewed under certain conditions by minors. Sex educational material, or materials depicting violence such as some nature documentaries, could potentially be filtered out by a 'blunt' ratings system. Depending on the technology used to establish the rating, this material may be withheld and may cause issues for some young people in researching or establishing a good understanding of an issue.

The technology employed for the ratings system therefore needs to be open and transparent, and to allow for human intervention should regulatory overreach occur. Despite the importance of restricting children's access to harmful content, freedom of expression should not be impeded where it doesn't compromise accepted standards of decency, to ensure that young Australians have access to material considered necessary for their educational goals.

A transparent review process should also be included in the RAS to prevent a situation where content which has been incorrectly rated harmful by the assessment process can be appealed to independent review body if appropriate.

---

6 https://www.aph.gov.au/Parliamentary_Business/Committees/House/Social_Policy_and_Legal_Affairs/Onlineageverification/Report/section?id=committees%2Freportrep%2F024436%2F72614#footnote105target

7 https://www.bbc.com/news/world-australia-56099523

6. What systems, methods and approaches do you consider effective, reasonable and proportionate for verifying the age of users prior to limiting access age-inappropriate material?

ACCAN's primary concern is that the age verification tests used by consumers are robust and cannot be manipulated by children under the age of 18. Age checking systems that involve self-declaration of age but do not require identification to prove authenticity are completely ineffective and use of credit cards as proof of identification are easy to circumvent.

A recent study by the researchers at Lero, the Science Foundation Ireland Research Centre for Software, found that children of all ages can completely bypass age verification measures to sign-up to social media apps including Snapchat, Instagram, TikTok, Facebook, WhatsApp, Messenger and Skype by simply lying about their age.[8]

Internationally we have seen failed attempts to introduce more effective online age verification systems, albeit under the GDPR which allows individual Member States some flexibility in determining the national age of digital consent for children between the ages of 13 and 16. The difficulties faced in imposing an effective and secure age verification process is illustrated by the UK government's scrapping of plans to enforce age checks on pornography websites under the *Digital Economy Act 2017* [9] after a major newspaper easily bypassed the age checker system with a fake email and credit card number.[10]

In fact, most of the age verification solutions that have been proposed have weaknesses and can either be circumvented or present privacy and security risks. For example, age recognition based on biometric factors such as facial features can be bypassed, as can voice recognition simply by using a voice recording. Online age verification involving a user submitting their mobile phone number, and then determining that a contract is associated with the phone number, is also ineffective. Although mobile phone contracts are restricted to individuals aged 18 years or above, children can easily input the mobile phone number of an older person – for example, a parent, guardian or older sibling - to gain access.

Lero researchers have recommended that providing mechanisms that deter a user from installing an app on a device on which they have previously declared themselves to be underage is currently the most sensible solution and the hardest to circumvent. However, this does not take account of the fact that often members of a household of different ages share the same device.

ACCAN is aware of other methods of age verification which could be extended to apply to the online services specified in the RAS. For example, confirming a user is listed on the Commonwealth electoral roll or has credit reporting information retained on Equifax's consumer credit bureau would indicate that the user is aged 18 years or above. Currently, however, Commonwealth electoral roll and credit reporting information can be used for anti-money laundering and counter-terrorism financing purposes, but not for other identity- or age-verification purposes.

---

[88] L. Pasquale, P. Zippo, C. Curley, B. O'Neill and M. Mongiello, "Digital Age of Consent and Age Verification: Can They Protect Children?," in *IEEE Software*, doi: 10.1109/MS.2020.3044872

[9] https://www.newscientist.com/article/2220220-uk-scraps-plan-to-enforce-age-checks-on-pornography-websites/#ixzz76gL6nOKe

[10] https://www.theguardian.com/society/2019/apr/19/uks-porn-age-verification-rules-can-be-circumvented-in-minutes

ACCAN submits that age verification schemes need proof, be it biometric data, Artificial Intelligence software or ID documentation, to be effective. However, we also acknowledge this approach comes with privacy and security risks and there is a need for a secure system of data sharing. The Digital Identity System, developed by the Digital Transformation Agency to give Australian people and businesses a single, secure way to authenticate their identity for the purpose of accessing government services online, could be of use here. However, ACCAN notes that it has previously expressed concern about the relaxation of the consumer-focussed privacy and security requirements set out in the DTA's Trusted Digital Identity Framework (TDIF) in the interests of attracting greater industry participation.

To minimise risk, any age verification system that collects and stores proof of identity data must only require the provision of minimum details to achieve a match and the data provided is used for the intended purpose only and is held securely. In addition, the data of consumers under the age of 18 should not be stored but should be deleted immediately after the verification process is complete.

Finally, age verification processes should continue after sign-up, to assess whether a user lied about their age on an ongoing basis and restrict access accordingly. Any age verification system must also be easy to use and fully accessible to all consumers including those with disabilities or from non-English speaking backgrounds.

7. Should the new RAS be prescriptive about the measures used to limit children's exposure to age-inappropriate material, or should it allow for industry to determine the most effective methods?

Under the UK's proposed age verification scheme under the *Digital Economy Act*, the BBFC took a 'principles-based' approach to certifying content providers' compliance with age verification requirements under the Act. This flexibility was intended to allow room for technological innovation and incorporation of new age verification techniques that were "both robust and easy to use for consumers" as technology continued to evolve.[11]

For example, recent developments in age-estimation software allows social and behavioural information from a social media account to verify age. Similarly, other advances in technology are enabling platforms and services to identify whether users are adults or children from behavioural and online signals. Handles or usernames, image tags, hashtag usage, gesture patterns, web history, content interaction, IP address, location data, device serial number, contacts – all can be used to measure what age-bracket a consumer might fall under. These signals are sometimes used by social media platforms, alongside third-party verification systems, to flag users who might be underage on their site.[12]

ACCAN agrees that in this respect, it would be appropriate for the RAS to be less prescriptive about the technology used to limit children's exposure to age-inappropriate material to allow emerging state of the art technology to be employed for the purposes of age verification.

However, in terms of the technical standard of age verification procedures that content providers must provide, ACCAN submits that an externally audited benchmark must be set that applies across the board. Allowing individual industry players to make their own assessments about the adequacy

[11] British Board of Film Classification, Submission to the Australian Government's *Inquiry into Age Verification for Online Wagering and Online Pornography*, October 2019, p. 11

[12] eSafety Commissioner, Submission to the Australian Government's *Inquiry into Age Verification for Online Wagering and Online Pornography*, October 2019, p. 8

of their age verification procedures is open to bias and may be driven by motives other than standards of decency - for example, cost saving or profit.

Additional Information

8. Is there any additional information eSafety should consider in drafting a new Restricted Access System declaration?

First, ACCAN agrees with the Office of the eSafety Commissioner that there is a need for independent auditing and monitoring of age-verification technologies. We also agree that the public should be made aware of the safeguards that are in place.[13]

Second, given the challenges faced in developing an age verification system that is effective and secure, restricted access systems need to be buttressed by other measures. For example, Lero recommends these measures to offer additional protection to children who have successfully bypassed age verification gateways and accessed apps intended for users who have reached the age of consent:

- Existing apps should ensure that a clear, concise and age-appropriate summary of the relevant parts of an app's Terms of Use is displayed to users who sign-up and declare their age to be under 18.
- Apps should apply the most restrictive privacy settings by default for any user that declares themselves to be under the age of 18. For example, photos, posts and messages should only be shared with "friends", location data should not be collected at all. It should also not be possible to override privacy settings without explicit parental consent.
- Despite the presence of a minimum age requirement, many underage users continue to use social and communication apps. Users must be incentivised to be honest about their age, with minimal data collected.[14]

Sincerely

Wayne Hawkins

Director of Inclusion

[13] https://www.aph.gov.au/Parliamentary_Business/Committees/House/Social_Policy_and_Legal_Affairs/Onlineageverification/Report/section?id=committees%2Freportrep%2F024436%2F72614

[14] Pasquale et al, op cit.