Submission to the eSafety Commission

on the discussion paper on the

Restricted Access System Declaration

17 September 2021

DIGITAL
RIGHTS
WATCH

Overview

Digital Rights Watch (DRW) welcomes the opportunity to submit comments to the eSafety Commission in response to the discussion paper on the Restricted Access System (RAS) Declaration. As an organisation working on the protection of digital rights, we are concerned regarding the impact of RAS upon individuals' and communities' rights, as well as adverse impacts on our collective privacy and digital security.

We note that the eSafety Commission has also called for evidence regarding the implementation of a 'roadmap' to a mandatory age verification (AV) regime relating for access to online pornography, and that submissions made to the RAS consultation may be considered in addition to evidence supplied to the AV call for evidence. As there is significant overlap regarding the concerns of the RAS and AV, we request that the eSafety Commission please also consider this submission with regard to the AV roadmap. Our team is available for further clarification or comment to this submission.

We are primarily concerned with the following:

- Practically all approaches to implementing a RAS will require the provision of personal information, which creates significant privacy and security risks,
- Mandatory AV may lead people of all ages to less safe and secure internet services in order to circumnavigate providing personal information,
- The administrative burden upon smaller Australian content hosts is likely to be unreasonable, and
- Most existing approaches to RAS/AV can be trivially bypassed, rendering them ineffective for the proposed objective.

For reference we would also like to share the submissions we have previously made regarding the Online Safety Act[1] as well as one provided to the Digital Transformation Agency regarding Digital Identity.[2]

Digital Rights Watch

Digital Rights Watch is a charity organisation founded in 2016 whose mission is to ensure that people in Australia are equipped, empowered and enabled to uphold their digital rights. We stand for Privacy, Democracy, Fairness & Freedom in a digital age. We believe that digital rights are human rights which see their expression online. We educate, campaign, and advocate for a digital environment where individuals have the power to maintain their human rights.[3]

[1] Digital Rights Watch submission to the Department of Infrastructure, Transport, Regional Development and Communication on the proposed *Online Safety Bill 2020*: https://digitalrightswatch.org.au/2021/02/18/submission-the-online-safety-bill/

[2] Digital Rights Watch submission to the DTA on proposed digital identity framework: https://digitalrightswatch.org.au/2021/07/30/submission-digital-identity/

[3] Learn more about DRW at https://digitalrightswatch.org.au

General remarks

Age verification (AV) and Restricted Access Systems (RAS) have been suggested for years but have repeatedly failed to be implemented or used due to their overreach, blunt approach, unreasonable impact upon individual's privacy, and creation of digital security risk.

At Digital Rights Watch, we are concerned that practically all approaches to implementing a RAS will require the provision of personal information that goes well beyond proof-of-age, which is an unreasonably invasive measure. Mandatory AV is likely to act as a deterrent for many adults accessing legal content, and may prompt people of all ages to less safe and secure internet services in order to circumnavigate providing personal information. The administration of such a system is also likely to be unreasonably burdensome for smaller Australian content hosts, pushing more content suppliers to move abroad. Finally, we are also concerned that many of the current approaches to AV are relatively easily bypassed, for example, by use of a Virtual Private Network (VPN).

The combination of these factors are likely to result in a system which is unduly invasive, creates new privacy and security risks, and is unlikely to be effective at preventing people under the age of 18 from accessing restricted content. We are concerned that the outcome will be a system that is not merely ineffective but actively harmful.

For this purpose we recommend an approach that prioritises making websites ensure that their content is more easily filterable by parental control software. This, combined with relevant education, would empower parents and children to manage access to pornography and other 'age-inappropriate' material, rather than imposing an invasive regime upon all Australians regardless of their age. The Commission may also wish to consider an approach which prioritises shifting the responsibility away from content providers and onto Internet Service Providers (ISPs), whereby parents and guardians providing a child with access to a device may request that their ISP filter the internet accordingly.

We note that the UK has previously attempted to implement a regulatory and policing regime for age-restricting access to pornography. Even before its implementation, the approach was criticised for having serious flaws and shortcomings, including the inability to actually significantly curtail young people's access to online pornography, as well as risks of privacy violations and harms to legitimate users' interests. In 2019 the plan was abandoned following years of technical challenges and pushback from privacy and security experts.[4]

Impact on young people

There is a significant amount of research into the complex connection between access to pornography and harmful outcomes for young people. While Digital Rights Watch does not have our own research in this area, we would urge the eSafety Commissioner not make the assumption that exposure to pornography is inherently harmful to young people. In fact, the

[4] 'UK drops plans for online pornography age verification system,' *The Guardian,* October 2019. Available at: https://www.theguardian.com/culture/2019/oct/16/uk-drops-plans-for-online-pornography-age-verification-system

association between exposure to pornography and harm has been contested by many experts in the realm of sexuality and young people.

For example, research in Croatia found no compelling evidence that pornography use is substanically associated with sexual risk taking among young people.[5] Research conducted in Switzerland found that exposure to pornography is not associated with risky sexual behaviours.[6] Even in research where an association between pornography and harmful or risky social outcomes is suggested, proposals that focus on harm reduction rarely propose complete restriction of sexually explict content, instead focusing on education and improved communication between children and adults.

In particular, we wish to highlight that restriction of access to sexually explicit material will disproportionately affect, and possibly harm, young LGBTQ+ individuals. Research has shown that young LGBTQ+ people often rely on the internet and pornography to gain sexual health information due to the lack of inclusive school sexual education programs, and as a counternarrative to dominant heteronormative experiences and media.[7]

Any approach to RAS/AV should consider the opinions of, and impacts upon young people, rather than a purely top-down approach. Research conducted in Australia showed young people generally do not support national-level filters of pornography, and would prefer school-based or national pornography education campaigns.[8]

Further, it is likely that ‘age-inappropriate material’ will apply to more than just pornogrpahic content, and may include sexual health information. We are concerned that a blanket approach to preventing access to ‘age-inappropriate material’ may restrict young people’s ability to access vital healthcare information, and lead to adverse health outcomes.

Preventing young people from accessing online pornography and other ‘age-inappropriate material’ is unlikley to meet community expectations among young people, and is also unlikely to mitigate perceived harms caused by such access without accompanying robust and inclusive sex education and resources for young people across all sexualities.

[5] ‘Revisiting the association between pornography use and risky sexual behaviors: the role of early exposure to pornography and sexual sensation seeking’, Sinković, M., Štulhofer, A. and Božić, J., *Journal of Sex Research*, Vol. 50 No. 7 (2013), pp. 633-641.

[6] ‘Associations between online pornography and sexual behavior among adolescents: myth or reality?’, Luder, M.T., Pittet, I., Berchtold, A., Akré, C., Michaud, P.A. and Surís, J.C., *Archives of Sexual Behavior*, Vol. 40 No. 5, (2011), pp. 1027-1035.

[7] ‘Young People, Sexual Literacy, and Sources of Knowledge,’ *La Trobe University*, October 2019. Available at: https://www.latrobe.edu.au/__data/assets/pdf_file/0011/1072973/Young-People,-Sexual-Literacy-and-Sources-of-Knowledge.pdf; ‘Young Australians' use of pornography and associations with sexual risk behaviours,’ *Monash University*, August 2017. Available at: https://research.monash.edu/en/publications/young-australians-use-of-pornography-and-associations-with-sexual

[8] ‘’Censorship is cancer’: Young people’s support for pornography-related initiatives,’ Lim, M., Roode, K., Davis, A. and Wright, C., *Sex Education,* (2020), pp 1-4.

Age restriction methods

The Online Safety Act requires that systems for restricting the access of people under 18 to 'age-inappropriate material' are in place from commencement of the Act, but it does not specify the requirements for how this should be implemented.

There are many technological approaches to age verification. We have identified and grouped the typical approaches below, including a high level overview of our concerns as they relate to privacy, security and digital rights.

1) **A requirement to provide identity documents to the service/platform that hosts the content, or to a third party service, either specifically for age verification, or more broadly as part of identity verification.**

It was only in March 2021 that the House of Representatives Standing Committee on Social Policy and Legal Affairs recommended that in order to have a social media account, individuals should be "required by law to identify themselves to a platform using 100 points of identification, in the same way a person must provide identification for a mobile phone account," as a measure to reduce online abuse.[9] The provision of government identity documents or biometric information to social media platforms was also suggested in August 2021 by the UK Children's Commissioner as a method to restrict access to online pornography.[10]

We are deeply concerned by these proposals, and the impact that such an approach would have upon individuals' right to privacy, their ability to remain anonymous online, and the security of their identity. **We strongly recommend that the eSafety Commission do not consider any proposal to require individuals to provide government-issued identity documents to content providers or digital platforms.**

The risk of identity theft in the event of a data breach whereby personal information is inappropriately or unlawfully accessed and leaked is significant. If the RAS were to require sites hosting sexually-explicit content to collect and hold identifying documentation, it is likely that they would become hacking targets, as datasets identifying those who watch pornography online has considerable blackmail value for cybercriminals. We remind the Commission of the leak of 30 million accounts when the adultery site, Ashley Madison, was hacked in 2015. The resulting harm caused by such sensitive information being inappropriately-accessed included several deaths by sucide.[11]

[9] 'Inquiry into family, domestic and sexual violence,' *House of Representatives Standing Committee on Social Policy and Legal Affairs*, March 2021, recommendation 30. Available at: https://parlinfo.aph.gov.au/parlInfo/download/committees/reportrep/024577/toc_pdf/Inquiryintofamily,domesticandsexualviolence.pdf;fileType=application%2Fpdf

[10] 'Social Media companies to be told to introduce tough age checks using passports or fingerprint analysis,' *The Telegraph,* August 2021. Available at: https://www.telegraph.co.uk/news/2021/08/30/social-media-companies-told-introduce-tough-age-checks-using/

[11] 'Ashley Madison suicides over web attack,' *BBC,* August 2015. Available at: https://www.bbc.com/news/technology-34044506

We also wish to emphasise the importance of maintaining the ability for people to be anonymous online. The suggestion that reducing anonymity would inherently reduce online harms is misguided. In fact, many vulnerable groups including victim-survivors of family violence rely on anonymity online to maintain their safety.[12] As such, any RAS or AV regime must not undermine the ability for people to be anonymous online, and must not require people to provide government-issued identity documents to digital platforms.

With regard to the prospect of using a third-party age-verification service, we wish to emphasise that there should be no information-sharing between the site hosting the restricted content, and the third party providing the age check. For instance, the site providing the restricted content should not be able to access any identification details or know who the person is, and the age verification service should equally not know which site the individual is trying to access, only that age verification is required.

Further, there should never be retention of age-verification data, including metadata logs. If this information were to be retained, it could remain possible to trace or link an identity to their online pornography-viewing habits and preferences, as well as any other 'age-inappropriate material' they may have accessed, which could reveal details about their sexual health or sexual practices. This is a flagrant invasion of privacy. Once an individual's age has been verified and they have been granted access, all records of the transaction should be permanently destroyed. There should be no way to retroactively link an individual's identity to the content they have accessed.

2) Verification of age based on user information being cross-checked in other databases that incorporate age-related information.

This approach generally relies on identity or age being validated against verification of another dataset in order to corroborate the information provided by an individual, such as the electoral roll, credit records, or drivers license databases. For example, Equifax suggested in 2019 that "age verification could involve confirmation that a user is listed on the Commonwealth electoral roll or has credit reporting information retained on Equifax's consumer credit bureau, either of which indicates that the user is aged 18 years or above."[13]

However, absence from any of these datasets does not necessarily mean that the individual in question is under the age of 18. We note that the vast majority of adults are either enrolled to vote (96%) and Equifax has estimated that 18 million Australian adults are listed on the customer credit bureau. Nonetheless, this still does not mean that an individual who is not in a database is by default under the age of 18.

We also have strong concerns about the process of cross-referencing information about individuals in datasets controlled by governments at various levels as well as the private

[12] See: 'Why Anonymity is Important,' *Digital Rights Watch,* April 2021. Available at: https://digitalrightswatch.org.au/2021/04/30/explainer-anonymity-online-is-important/

[13] 'Inquiry into age verification for online wagering and online pornography,' *Standing Committee on Social Policy and Legal Affairs,* 2019-2020. Section 2.103. Available at: https://www.aph.gov.au/Parliamentary_Business/Committees/House/Social_Policy_and_Legal_Affairs/Onlineageverification/Report/section?id=committees%2Freportrep%2F024436%2F72614

sector, and the possibility of inappropriate information sharing or linking across disparate datasets.

Finally, we do not believe that this approach would meet community expectations regarding the use of their personal information. When individuals enrol to vote, register for a drivers license, or use a credit card, they have not provided their personal information for the purpose of validating access to pornography.

3) **Use of biometric software, either by way of facial recognition or 'age estimation software' that uses photos, vidoes, or a live stream to estimate age.**

The use of facial recognition technology to verify an individual's age by means of checking their identity against a government-issued identity document represents a significant and disproportionate invasion of privacy, and as such, is not an appropriate approach to restricting access to particular online content.

In the 2019 'Protecting the Age of Innocence' inquiry, the Department of Home Affairs suggested the use of facial recognition technology by way of its Facial Verification Service (FVS), which it proposed could then be cross-checked with other identity documentation that Home Affairs already holds.[14] However, this is subject to the passage of the *Identity Matching Services Bill 2019,* which we note has received significant public backlash and criticism from privacy and security experts.

The prospect of the Department of Home Affairs utilising facial recognition for the purpose of regulating access to online pornography and other 'age inappropriate material' is unacceptable. No government department, but especially not the one which also contains policing and intelligence agencies within its profile, should be able to associate an individual's biometric data with their sensitive online habits. This would be a gross misuse of government power and an unreasonable overstep into people's personal lives.

We also note that current facial recognition software still exhibits racial and gendered biases, and that by relying on such technology, a RAS may unreasonably prevent an individual who is over the age of 18 from accessing content online, should their face not be recognised by the facial recognition system.

By contrast, age estimation software may offer a less privacy-invasive solution, on the condition that no personal information (including biometric information) is collected or retained. However, we would note that the accuracy of age estimation software is questionable at best, and therefore may result in an unacceptable margin of error.

4) **Age screening based on requiring users to self-declare, such as through stating their date of birth or ticking a box to state they are over the age of 18.**

[14] 'Inquiry into age verification for online wagering and online pornography,' *Standing Committee on Social Policy and Legal Affairs,* 2019-2020. Section 2.111. Available at: https://www.aph.gov.au/Parliamentary_Business/Committees/House/Social_Policy_and_Legal_Affairs/Onlineageverification/Report/section?id=committees%2Freportrep%2F024436%2F72614

Many age-restricted online content already employs this method of age restriction, such as when accessing online stores which sell alcohol. While this approach is the least invasive and presents the least privacy and security risk, its efficacy is also minimal.

Digital Identity

We note that there have also been suggestions to use the Government's Digital Identity Program, including the Digital Transformation Agency's (DTA) Trusted Digital Identity Framework (TDIF) to support an online age-verification scheme.

The DTA has said that Digital Identity could be used to verify identity attributes, including age, for the purpose of accessing age-restricted sites: "Such sites would only receive the information required to confirm the user meets the age requirements of the service. Other information could potentially be provided, but this would be consent based to ensure the [user's] privacy is protected." In our latest response to their proposed measures, we recommended the DTA to:[15]

- Prioritise an update to the Privacy Act and the precedent it may set for privacy.
- Not integrate biometric data into the TDIF.
- Ensure that the digital identity framework remains truly voluntary.
- Maintain analogue pathways for individuals to interact with, and use, services.
- Ensure that there are easy ways to alter consent, and delete or alter data.
- Prohibit use of digital identity data for enforcement purposes.

Given the current shape of Australia's approach to digital identity and the lack of privacy protections and security safeguards, we do not support the use of the Government's Digital Identity Program, including the TDIF, for age verification. While there are existing approaches by a select few other countries (most located in the EU) who use government ID to age verify, the system is designed around privacy and uses a token access, which is a very different approach than the one under consideration in Australia. It would be highly inappropriate, and actively harmful for many vulnerable communities, for the government to have any ability to collect data regarding the online pornography viewing habits of adults in Australia.

Conclusion

The RAS and mandatory AV regime for access to online pornography and other 'age-inappropriate material' represents an unreasonable level of intrusion into individuals' privacy. When purchasing sexually explicit material offline, this transaction is generally anonymous, even where proof of age is required, as no identifying information is retained.

Given that there are ongoing concerns regarding the Australian Government's implementation of its Digital Identity Scheme, alongside significant concerns regarding the broad information-sharing powers under consideration in the *Data Availability and*

[15] Digital Rights Watch submission to the DTA on proposed digital identity framework: https://digitalrightswatch.org.au/2021/07/30/submission-digital-identity/

Transparency Bill 2020, any RAS or AV scheme which enables personal information to be collected, stored, and possibly disclosed or linked with other data, is unacceptable.

While we empathise with some of the concerns regarding people under 18 accessing pornographic materials, we do not see RAS/AV as an appropriate solution. There is no simple 'fix' to the challenge of age verification online. Yet, we note that the passage of the Online Safety Act requires that a system be in place. As such, we strongly suggest that the eSafety Commissioner opt for the least privacy-invasive approach, and that this be layered with other, non-technical approaches to address the perceived harms caused to young people from exposure to online pornography and other 'age-inappropriate material', including an emphasis on education.

Our recommendations

- Rather than implementing an invasive regime for all adults in Australia, we would prefer to see an approach that prioritises making websites ensure that their content is more easily filterable by parental control software, as well as leveraging the ability for ISPs to filter content on specific devices to be used by children.
- Prioritise education and communication, rather than trying to find a technological solution. Using a technological appraoch to prevent young people from accessing online pornography is unlikley to mitigate the perceived harms without accompanying robust and inclusive sex education and resources for young people across all sexualities.
- The RAS should under no circumstance enable the ability for government agencies or private companies to track or link an individual's identity with their online pornography viewing habits, or any other 'age inappropriate material' they may access.
- The RAS should not be prescriptive about the measures used to limit children's exposure to 'age inappropriate material,' however it should require safeguards against the use of certain approaches and technologies, including:
    - Prohibit the use of facial recognition technology or other collection of biometric data
    - Prohibit the association of identity with online pornography viewing habits, for instance, by way of prohibition of content providers from collecting identity documents, and conversely, prohibition of any third-party age verification services from collecting information regarding the content being accessed.

Contact

Samantha Floreani | Program Lead | Digital Rights Watch | samantha@digitalrightswatch.org.au