Submission to the eSafety Commission

on the draft

Restricted Access Systems Declaration 2021

23 November 2021

Overview

Digital Rights Watch (DRW) welcomes the opportunity to submit comments in response to the draft Restricted Access Systems (RAS) Declaration. We recognise there are unique challenges posed by the ubiquitous nature of the internet, and the legitimate interest of the Australian government to promote safer online services to individuals across Australia. However, as an organisation working to protect our collective digital rights, we are concerned about the impact of the declaration on individuals' and communities' rights, as well as adverse impacts it may have on our privacy and collective digital security.

We note that the eSafety Commission is also in the process of developing a roadmap to a mandatory age verification (AV) regime which is set to cover access to online pornography. 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,
- Age verification requirements may lead people of all ages to less safe and secure internet services in order to circumnavigate providing personal information,
- Most existing approaches to RAS/AV can be trivially bypassed, rendering them ineffective for the proposed objective.

The draft RAS declaration places an undefined responsibility upon industry to determine 'reasonable steps' to verify a user's age. There is currently no widely accepted 'good' approach to implementing safe and effective age verification. In fact, most have been shown to create significant privacy and security risks.

For reference we would also like to share the submissions we have previously made on the RAS discussion paper[1], our initial submission on the proposed Online Safety Act[2] as well as one provided to the Digital Transformation Agency regarding Digital Identity.[3]

Digital Rights Watch

DRW 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.[4]

---

[1] Rights Watch submission to the eSafety Commissioner on the Restricted Access Systems (RAS) discussDigitalion paper: https://digitalrightswatch.org.au/2021/09/21/submission-restricted-access-system/

[2] 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/

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

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

General remarks

Age Verification (AV) and Restricted Access Systems (RAS) have been considered in the past but have failed to be implemented due to their overreach, blunt approach, unreasonable impact upon individual's privacy, and the creation of adverse digital security risks.

We are concerned that any of the existing approaches to implementing a RAS will require the provision of personal information that goes well beyond proof-of-age. Despite the significant challenges to implementing age verification in a way that is both effective as well as minimising privacy and security risks, we are concerned that the draft RAS Declaration in its current form places an unreasonable amount of responsibility upon providers to determine the 'reasonable steps' to meet the age confirmation requirements of Section 8.

We wish to reiterate from our previous submission that 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. Further, we remain 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 in data collection, creates new privacy and security risks by holding information on individuals, and yet is unlikely to be effective at preventing people under the age of 18 from accessing restricted content. We are therefore concerned that the outcome will be a system that is not simply ineffective but actively harmful.

Of the available solutions, we would recommend an approach that prioritises making websites ensure that their content is more easily indexed for 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 impose an invasive age verification regime upon all Australians regardless of their age.

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.[5]

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. In fact, the association between

[5] '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

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.[6] Research conducted in Switzerland found that exposure to pornography is not associated with risky sexual behaviours.[7] 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 thereby create harm for, 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.[8]

We are concerned that the draft RAS Declaration has not adequately considered the experiences of, and impacts upon, diverse groups of young people. Research conducted in Australia showed young people generally do not support national level filters for pornographic content, and would instead favor school-based or national-level pornography education campaigns.[9]

Further, we remain concerned that this scheme may, in practice, result in restricting access to material beyond that which is pornographic, and may include valid artistic expression as well as 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.

---

[6] '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.

[7] '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.

[8] '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

[9] ''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.

The proposed approach in the draft RAS Declaration

Section 7 - Provision of warnings

This section requires providers to give applicants a warning about the nature of the material that they are applying for access to, as well as safety information "about how a parent or guardian may control access to relevant class 2 material by persons under 18 years of age".

While we appreciate the objective of providing warnings to applicants under Section 7(a) and generally support this proposal, it is not clear to us who the 'safety information' under s 7(b) is supposed to be for, and how it will be an effective means of harm reduction if delivered at this point in the application process. The wording of Section 7(b) suggests that the 'safety information' is specifically for parents and guardians, however we question whether the way this will be implemented in practice will be an effective measure for the purported goal of educating parents and guardians.

To highlight the challenges with such an approach, we submit the following three scenarios:

1) **A person <u>under</u> the age of 18 attempts to apply for access.**
   Providing a person under 18 with safety information designed for parents/guardians does not make sense. Further, should the scheme be effective, the underage applicant will be denied access, and render the provision of information at this point in the process irrelevant.

2) **A person <u>over</u> the age of 18 who does <u>not</u> have children attempts to apply for access.**
   Requiring providers to show all adults seeking to legally access material with safety information designed for parents/guardians will result in many adults being provided with information that is irrelevant to them. This may be an acceptable annoyance should the mechanism be effective at education and behavioural change overall, yet it is not clear that that would be the case.

3) **A person <u>over</u> the age of 18 who <u>does</u> have children attempts to apply for access.**
   Even in cases where the safety information actually reaches the desired audience, providing parents or guardians with safety information regarding how to control access to such material while they are in the process of applying for access to relevant class 2 material is unlikely to be an effective moment for educational benefit. Adults who care for children may reasonably wish to access relevant class 2 material for their own personal consumption, which has no relevance to their role as a parent.

We appreciate the educational intention of Section 7, and support the proposal to provide warnings to viewers before accessing content. We also, in principle, support providing parents and guardians with safety information regarding how to control access to sensitive online material by people under the age of 18. However, we are skeptical that the approach of Section 7(b) in providing safety information "to the applicant" will lead to effective education outcomes or harm reduction.

- **Recommendation 1**
  Remove Section 7(b) from the declaration, as it is unlikely to be an effective means of harm reduction. The eSafety Commissioner is best-placed to provide such safety information to parents and guardians, not providers.

- **Recommendation 2**
  As an alternative to Recommendation 1, alter the wording of Section 7(b) to clarify that providers are not required to provide safety information "to the applicant", but to offer such information on their website for parents or guardians to access, should they seek it. The content of the safety information should be made accessible to industry in guidance developed by the eSafety Commissioner.

- **Recommendation 3**
  Prioritise education and communication at meaningful and effective points in time, delivered in appropriate ways, rather than trying to find a technological solution. Using a technological approach 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.

Section 8 - Confirmation of age

Section 8 requires an "access-control system" to incorporate reasonable steps to confirm that an applicant is of at least 18 years of age. The accompanying explanatory statement states that this is to ensure "providers must do more than simply accept a declaration of age".[10] The inclusion of "reasonable steps" makes this subsection non-prescriptive, leaving room for service providers to determine a range of age-verification methods.

While we appreciate the intention to allow for flexibility, we are concerned that Section 8(1):

1) places an unreasonable burden on providers to determine the best approach to implement age verification, which is a long-standing technical and ethical challenge to which there is no readily accepted 'good' solution, and
2) creates a risk that some providers may implement age verification solutions which present an unreasonable privacy and security risk to individuals.

We support the RAS not being prescriptive about the specific measures taken, but it should include guidance on what would be expected to be reasonable, as well as the requirement for safeguards against the use of certain approaches and technologies, including facial recognition technology or other collection of biometric data. It should also prohibit any association of identity with online pornography vieiwing habits.

The accompanying explanatory statement states:

> *"Reasonable steps may be established by transaction type – use of a credit card where content is fee-based, for instance. Other reasonable steps might link the*

[10] Draft RAS Explanatory Statement, page 8, as at 13 November 2021, https://www.esafety.gov.au/about-us/consultation-cooperation/restricted-access-system#download-the-draft-ras-declaration-and-explanatory-statement

application process to an already-validated age-restricted platform, allow provision of other identity related information, or allow applicants to use a token generated during another age confirmation process."[11]

In our previous submission on the discussion paper of the RAS Declaration, we highlighted our significant concerns regarding the privacy and security risks associated with various age verification implementation methods. Proposals to "link the application process to an already-validated age-restriction platform" or to "allow provision of other identity related information" are examples of approaches that are likely to create unreasonable privacy and security risk. We have included an overview of the common approaches to age-verification and the digital rights considerations in Appendix One, as well as concerns regarding the use of Digital Identity in Appendix Two to this submission.

The explanatory statement goes on to note:

> *"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."*[12]

While we appreciate the emphasis on privacy, we are concerned that this expectation is only contained within the explanatory statement, and not within the RAS Declaration itself.

- **Recommendation 4**
  Elevate the expectation that age confirmation methods should be privacy-preserving to the legislation, not the explanatory statement. It should also be made explicit in the legislation that age confirmation should not involve identity verification, as is contained in the explanatory statement.

- **Recommendation 5**
  It is appropriate for the RAS Declaration to be non-prescriptive about specific measures, however, it should require safeguards against the use of certain approaches and technologies, such as:
  - 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 prohibiting content providers from collecting identity documents, and prohibiting third-party age verification services from collecting information regarding the content being accessed.

[11] Draft RAS Explanatory Statement, page 8, as at 13 November 2021, https://www.esafety.gov.au/about-us/consultation-cooperation/restricted-access-system#download-the-draft-ras-declaration-and-explanatory-statement
[12] Draft RAS Explanatory Statement, page 8, as at 13 November 2021, https://www.esafety.gov.au/about-us/consultation-cooperation/restricted-access-system#download-the-draft-ras-declaration-and-explanatory-statement

Section 9 - Limiting access to relevant class 2 material

Section 9 requires that an “access-control system” must only provide access to class 2 material if it has met the requirements of sections 6, 7 and 8, or, if the applicant has been provided with a **Personal Identification Number** to confirm that they have previously met the requirements.

Many small providers may not fall under the cover of the *Privacy Act 1988*, and therefore not be required to meet the privacy protections contained in the Australian Privacy Principles (APPs), including restrictions on collection, use, and disclosure of personal information. In order to meet the requirements of the draft RAS Declaration, including Section 9, providers may opt to collect and store personal information of individuals in order to be able to confirm if a user has previously met the requirements of sections 6, 7 and 8. Compelling providers to collect and store personal information linked to a Personal Identification Number without being required to also meet the requirements of the APPs opens individuals up to significant and disproportionate privacy risk.

- **Recommendation 6**
  Explicitly prohibit providers from developing a system which logs, records or otherwise documents individuals’ access to, and viewing habits of relevant class 2 material. Given the sensitive nature and value of such information, this kind of database would create significant privacy risk for individuals, and is likely to also create considerable digital security risk for providers by positioning them as targets for malicious attacks.

- **Recommendation 7**
  Include explicit language in the Declaration that prohibits providers from collecting, using, storing, or disclosing personal information of visitors applying for access to relevant class 2 material that is not relevant or necessary for the purpose of providing access.

- **Recommendation 8**
  The RAS should also preclude any/all 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.

Conclusion

On principle, the requirement to verify age to access relevant class 2 material represents an unreasonable level of intrusion in individuals’ privacy. For instance, when purchasing sexually explicit material offline, this transaction is generally anonymous, even where proof of age is required, as no identifying information is retained. It is extremely challenging, if not impossible, to retain this level of anonymity while also meeting the requirements of age verification online.

The draft RAS Declaration in its current form places an immense burden upon providers to determine how to implement age verification mechanisms, despite the lack of any established 'good' approach to doing so. For smaller providers, this presents an immense administrative burden, while also creating significant privacy and digital security risk due to the small business exemption under the *Privacy Act*.

Given that there are ongoing concerns regarding the Australian Government's implementation of its *Digital Identity Scheme*, alongside significant concerns regarding the broad data sharing powers under consideration in the *Data Availability and Transparency Bill 2020*, we noted in our previous submission on the RAS discussion paper that "any RAS or AV scheme which enables personal information to be collected, stored, and possibly disclosed or linked with other data, is unacceptable." We wish to reiterate this concern with regard to the draft RAS Declaration. The draft declaration lacks privacy and security protections to mitigate the risks that this scheme will create.

While we empathise with some of the concerns regarding people under 18 accessing pornographic materials, we do not see the current 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 some amendments be made to the draft RAS Declaration, to mitigate the possible harms arising from the privacy and digital security risks.

Appendix One: Age restriction methods and digital rights

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.

The draft RAS requires providers to implement an "access-control system" that must incorporate reasonable steps to confirm that that applicant is at least 18 years of age, but it also does not specify the kinds of "reasonable steps" that providers must take.

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.[13] 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.[14]

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 RAS Declaration does not allow for any requirement for 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 targets for malicious actors. We remind the Commission of the leak of 30 million accounts when the adultery site, Ashley Madison, was hacked in 2015. The

[13] '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

[14] '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/

resulting harm caused by such sensitive information being inappropriately-accessed included several deaths by sucide.[15]

We also wish to emphasise the importance of maintaining the ability of individuals 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.[16] 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 an 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."[17]

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

---

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

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

[17] '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

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 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 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 restricted material online.

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 any 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.[18] 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.

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.

---

[18] '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

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.**

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 smallest privacy and security risk, its efficacy is also minimal.

Appendix Two: 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:[19]

- 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.

Contact

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

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