Digital Media Research Centre

QUT DMRC Submission to the Inquiry into the Internet Search Engine Services Online Safety Code and the under 16 social media ban

SUBMITTED BY
QUT Digital Media Research Centre
Building Z9, Creative Industries Precinct
Kelvin Grove, QLD, 4059

QUT Digital Media Research Centre

Overview

As a leader in social media, communication, digital humanities, and social science research globally, the Digital Media Research Centre (DMRC) welcomes the opportunity to make a submission to the *Inquiry into the Internet Search Engine Services Online Safety Code and the under 16 social media ban*.

Australia stands at a crossroads.

The rush to impose blunt technical age barriers risks transforming the open Internet from a civic space into a gated enclosure, ceding ever more power to the very surveillance-capitalist platforms whose practices already threaten privacy, autonomy, and safety.

True safety cannot be engineered through compulsory ID checks or online profiling. These are not neutral safeguards, but mechanisms that normalise mass data capture and deepen the dominance of a handful of global corporations.

Policies built on technological determinism and deficit framing mistake the problem and magnify the harm: treating every user as both suspect and victim while leaving the true underlying social and commercial drivers of online risks untouched.

Based on the detailed feedback we provide in this submission, we make the following high-level recommendations.

1. **Privacy-Preserving Safety**

   Instead of building or mandating systems that require the mass collection of sensitive data, policymakers should prioritise privacy-preserving approaches and safety by design. This includes strengthening baseline privacy protections for all users, limiting the collection of data by platforms, enforcing content standards where appropriate, and focusing on education that empowers everyone to manage online risk.

2. **Regulate Business Models, Not Identities**

   Policymakers should redirect attention towards regulating the business models of digital platforms, not expanding them. Limiting data collection, ensuring transparency of algorithmic profiling and content moderation, and enforcing meaningful rights to data access and deletion are more effective strategies than mandating and encouraging new layers of surveillance.

3. **Recognise Technical Limits**

   Technical interventions for age-gating access to digital services should be recognised as blunt instruments, useful only in exceptionally limited circumstances. Policymakers must avoid overpromising on what technical filters can achieve. Resources would be better spent supporting the co-design of safe and positive online spaces with young people themselves.

4. **Invest in Co-designed Education and Support**

   The government should prioritise co-designed education programs and technologies that empower young people and the wider community. Instead of seeking to protect children *from* the digital environment, policy should focus on protecting them *within* it. This means investing

in high-quality, free, age-appropriate digital products and services, co-created with young people, rather than relying on technical bans.

5. **Independent, Community-Centred Oversight**

   Establish an oversight framework that centres independent, academic, and community-based expertise rather than expanding government or industry control. This should include resourcing independent researchers with access to platform data, embedding civil society voices in decision-making, and supporting community-led digital literacy and safety programs as part of ongoing evaluation. Oversight should be judged by outcomes in practice, not the mere existence of technical compliance mechanisms.

6. **Learn from Global Best Practice**

   Australia should position itself as a leader in evidence-based, socially-grounded online safety policy. By learning from the failures of purely technical approaches overseas and aligning with global best practice in education and civic engagement, we can deliver outcomes that are both effective and respectful of rights.

7. **Affirm Children's Rights and Digital Citizenship**

   The Committee should explicitly recognise that online safety is not just a technical problem. It is a civic challenge requiring investment in people, not only infrastructure. Australia can lead by example, choosing education and empowerment over surveillance and exclusion.

The Digital Media Research Centre urges the Committee to resist a path that trades fundamental rights for an illusion of control. Protecting young people online demands evidence-based, human-centred solutions: education, civic investment, and privacy-by-design approaches that build resilience without sacrificing freedom.

Yours sincerely,

Professor Daniel Angus FQA
Director, Digital Media Research Centre, Queensland University of Technology

QUT Digital Media Research Centre

Responses to Terms of Reference

a) privacy and data protection implications of age verification;

The concept of employing automated processes and digital profiling to manage access to online spaces under the guise of 'protection' is fundamentally misconceived.

We share concerns that the Australian Age Assurance Technology Trial (AATT) has been undermined by structural conflicts of interest and transparency failures[1]. Central among these is that the body appointed to assess and certify age-verification technologies, the Age Check Certification Scheme (ACCS), is itself closely enmeshed within the industry that stands to gain enormous revenue from mandatory deployment of age assurance technologies. This raises acute concerns: how can a process be impartial when those making evaluations are the same commercial actors likely to profit from nationwide regulation and compulsory adoption of the services of their peers?

Despite the AATT report attempting to downplay the significance and scale of unresolved issues[2], **any fair reading must conclude that age assurance technologies continue to raise serious privacy, security, accuracy, and inclusivity concerns**[3].

In practice, age assurance will most likely require individuals, including children, to submit to profiling, either through platforms' own collection and use of sensitive personal data such as web histories and other online trace data; by submitting additional personal documents such as driver's licences, bank cards, or passports; or, by providing biometric data such as facial scans. Truly privacy-preserving methods exist but these are rare and rarely deployed at scale.

The provision of personal data creates valuable and exploitable targets for criminal actors, hostile states, or malicious insiders. As Australia has seen with high-profile breaches of Optus, Medibank, and Qantas, leaks of identity documents, biometric and online trace data create long-term, irrevocable harms for individuals and their families. **Australia cannot afford to normalise the routine surrender of such highly sensitive personal information.** These breaches also serve as stark reminders of the hubris in believing that large, well-funded teams with sophisticated IT systems are immune from attack; they show that any retained digital data can be only seconds away from compromise.

Mandatory age assurance techniques may require users to either verify their age every time they access content, save their details for future access, or use existing device or account-level flags (i.e. bank details). In all cases, the net result is the expansion and further normalisation of digital data trails, making Australians more vulnerable to identity theft and fraud, and inviting continued and unwelcome intrusions into their private online activities. It is difficult to see how these risks can be reconciled with the government's obligations under privacy law to promote data minimisation and proportionality.

---

[1] Electronic Frontiers Australia. (2025, August 14). EFA challenges claims of age assurance technology trial success. https://efa.org.au/preliminary-findings-of-the-australian-governments-age-assurance-technology-trial/

[2] Taylor, J. (2025, August 19). Key stakeholders in Australia's social media age assurance trial frozen out amid media leaks and resignations. *The Guardian*. https://www.theguardian.com/media/2025/aug/19/australia-age-assurance-trial-social-media-ban-leaks-resignations

[3] Given, L. (2025, September 1). Australia's government says social media age checks "can be done", despite errors and privacy risks. *The Conversation*. https://theconversation.com/australias-government-says-social-media-age-checks-can-be-done-despite-errors-and-privacy-risks-264257

QUT Digital Media Research Centre

The situation is further complicated by the release of the new Online Safety Codes alongside the social-media age ban. These overlapping initiatives muddy the waters regarding the purpose and scope of age verification, asking Australians to hand over increasing amounts of personal information without a clear or proportionate justification. By conflating two distinct processes, policy is drifting toward a single, expansive surveillance regime pursued in the name of loosely defined “safety” and “harm” reduction. Such conflation obscures accountability and makes it impossible for the public to judge whether data demands are necessary, proportionate, or aimed at achieving the same goals.

As one key example of potential conflation, Internet search became an everyday application alongside the creation of the World Wide Web, grounded in an information ecosystem meant to foster accessibility and the free flow of knowledge. Search engines serve as essential intermediaries between information producers and seekers and, crucially, have never strictly required logins or identity verification by default, mirroring offline public information systems such as libraries.

Major providers have applied proportionate safety-by-design measures: default SafeSearch settings that blur explicit images and attempt to surface reliable health resources for high-risk queries. These controls are sensible and widely supported but can still lead to overzealous blocking and restriction so should be monitored with care; and we renew our call for legislated access to platform data for independent, accredited researchers.

The challenge is ensuring that the next regulatory step, mandating formal age assurance, does not become another avenue for large search companies, already known for extensive data harvesting, to expand their collection activity. The obligation should be the opposite: for platforms to minimise the data retained and to require strict limits on how any age-verification signals are stored, shared, or linked to general user profiles.

The key potential for harm lies in connecting real-name or identity details with the intimate and often sensitive record of search queries. **Regulation should explicitly require that any age-verification data remain strictly segregated from search logs.** Without such guardrails, a policy intended to protect could inadvertently entrench more invasive tracking, running counter to the privacy-by-design goals of Australia’s long-delayed Privacy Act reforms.

The policy premise also warrants closer scrutiny. Adolescents are naturally sexually curious, and evidence shows that thoughtful, guided sexuality education, not blanket restriction, is the most effective way to support healthy development and reduce harm[4]. Much of the advocacy behind universal age-assurance conflates the frequency of pornography exposure with demonstrated harm, a framing often advanced by ideologically motivated anti-pornography campaigns[5]. When policy treats all sexual content as inherently damaging, it risks importing a moral agenda under the guise of child protection and ignoring the complexity and science of adolescent sexual exploration.

From a digital inclusion standpoint, not all Australians have access to the necessary identity documents to satisfy age verification systems. It is well understood that low-income families, refugees, and other marginalised groups may lack passports, driver’s licences, and bank details.

---

[4] Davis, A. C., Wright, C. J., Murphy, S., Dietze, P., Temple-Smith, M. J., Hellard, M. E., & Lim, M. S. (2020). A Digital Pornography Literacy Resource Co-Designed With Vulnerable Young People: Development of “The Gist.” *Journal of Medical Internet Research*, *22*(6), e15964. https://doi.org/10.2196/15964

[5] Dawson, K., Nic Gabhainn, S., & MacNeela, P. (2019). Toward a Model of Porn Literacy: Core Concepts, Rationales, and Approaches. *The Journal of Sex Research*, *57*(1), 1–15. https://doi.org/10.1080/00224499.2018.1556238

QUT Digital Media Research Centre

In these cases, age verification does not simply delay access; it may exclude entire populations from digital participation. Shared device use, common in families with limited resources, further complicates implementation, creating additional burdens on already stretched community organisations such as libraries and community centres[6]. These contexts demand close attention.

The burden is also already felt acutely by smaller Internet content services, which may host material with mature themes for legitimate artistic, educational, or community purposes. Unlike large multinational platforms, these services rarely have the resources or capacity to implement complex age verification mechanisms, nor the skills or desire to handle sensitive user data responsibly. Imposing such obligations places them in impossible territory, exposing them to compliance risks and liabilities they cannot manage[7].

The decentralised social network Bluesky, widely regarded as a pro-social alternative to platforms like X (formerly Twitter) that are rife with hate speech, has publicly noted that the engineering and legal costs of mandatory age-gating in certain jurisdictions are prohibitive for a start-up[8]. Similar concerns are echoed across the wider Fediverse—a decentralised network of interconnected, often volunteer-run social servers (such as Mastodon) that communicate via open protocols rather than a single corporate platform—where many small, volunteer-run servers simply cannot absorb the expense or liability of large-scale age verification[9]. The effect is to discourage participation, diminish diversity, and erode one of the fundamental benefits of the Internet: that it allows anyone, regardless of scale or status, the ability to participate in and contribute to culture.

From a rights-based perspective, the danger is clear. These systems transform all Australians from digital citizens into perpetual suspects, forced to prove their legitimacy before they can participate in ordinary online life. These barriers to information add an unnecessary layer of costs for all stakeholders, without clear justification or evidence of their effectiveness at dealing with deeper cultural and social issues. These moves risk exposing the entire population to greater privacy harms, and access to vital information becomes contingent upon the capabilities of private entities: particularly multinational corporations, but also smaller start-ups and minor platforms. In our assessment, mandatory age assurance fails any dispassionate risk assessment when all relevant factors are weighed.

Recommendation: Instead of building or mandating systems that require the mass collection of sensitive data, policymakers should prioritise privacy-preserving approaches and safety by design. This includes strengthening baseline privacy protections for all users, limiting the collection of data by platforms, enforcing content standards where appropriate, and focusing on education that empowers everyone to manage online risk.

---

[6] Notley, T., & Aziz, A. (2024). The unjust burden of digital inclusion for low-income migrant parents. *Policy & Internet*, *16*(2), 428-442. https://onlinelibrary.wiley.com/doi/full/10.1002/poi3.383

[7] Shyy, S. (2019). The GDPR's Lose-Lose Dilemma: Minimal Benefits to Data Privacy & Significant Burdens on Business. *Uc davis bus. lj*, *20*, 137. https://blj.ucdavis.edu/archives/20/2/gdprs-lose-lose-dilemma-minimal-benefits-data-privacy-significant-burdens-business

[8] Buckley, M. (2025, September 5). Age verification is a windfall for Big Tech-and a death sentence for smaller platforms. *Electronic Frontier Foundation*. https://www.eff.org/deeplinks/2025/09/age-verification-windfall-big-tech-and-death-sentence-smaller-platforms

[9] Struett, T., Sinnreich, A., Aufderheide, P., & Gehl, R. (2024, November 9). Can this platform survive? Governance challenges for the fediverse. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4598303

QUT Digital Media Research Centre

b) the expansion of corporate data collection and user profiling capabilities enabled by code compliance requirements;

Requiring platforms to comply with age verification will expand, not reduce, their incentive to profile users more deeply. These new codes and legislation create conditions where global technology companies will collect, verify, and store (whether pre-emptively or necessarily) additional categories of personal data. This is not a small or incidental change: it represents a fundamental expansion and normalisation of surveillance practices. **It is no defence to argue that because many platforms already possess data that *could* be used to infer age, government-mandated verification is harmless.** Those practices remain problematic precisely because Australia has yet to complete long-promised Privacy Act reforms (specifically Tranche 2) that would begin to rein in invasive data harvesting across the board. The appropriate response is to strengthen those privacy protections for everyone, not to legitimise and entrench the very profiling that requires urgent regulation.

Compliance with these requirements may encourage companies to develop new 'shadow profiles' based on age, identity documents, biometric scans, and behavioural patterns. Such profiles can be combined with existing data to refine advertising, recommendation systems, and content moderation. The long-term result is a deepening of the surveillance economy that already undermines public trust in digital platforms.

This 'safety paradox' is well understood[10]. Measures intended to protect children often expand the very practices, data extraction, profiling, and behavioural manipulation, that create risks in the first place. Teens, meanwhile, are drawn to online spaces because they offer a degree of privacy and autonomy rarely available elsewhere; these spaces often serve as vital safe harbours, especially for those exploring non-normative identities[11]. In effect, our collective participation online is becoming increasingly conditional on submitting to intensified forms of monitoring —it should not be so.

Australian citizens should not be required to surrender more personal data to opaque multinational companies as a precondition for accessing essential digital services. Doing so contradicts the need for increased protection of privacy and further entrenches the market dominance of very large online platforms. It is a solution that prioritises corporate control over our fundamental digital rights.

Even more concerning is that this approach runs directly counter to the very harms that motivated moves to legislate age restrictions in the first place. **Concerns about addictive design, infinite scrolling, and manipulative recommendation systems cannot be addressed by expanding the supply of private and sensitive data to the very companies whose business models rely on exploiting it.** On the contrary, meaningful progress on these issues would require *reducing* the flow of personal data, not mandating more.

This paradox reveals why rushed legislation, drafted without meaningful input from independent experts, is so dangerous. In seeking to act quickly, government risks making the problem worse by bolstering the power of platforms rather than constraining it, and by killing off creative alternative products that embed safety by design principles. Careful, evidence-based policymaking must replace

---

[10] Wisniewski, P. (2018). The privacy paradox of adolescent online safety: A matter of risk prevention or risk resilience?. *IEEE Security & Privacy*, *16*(2), 86-90. https://ieeexplore.ieee.org/document/8328977
[11] boyd, d. (2014). *It's complicated: The social lives of networked teens*. Yale University Press. https://www.danah.org/books/ItsComplicated.pdf

QUT Digital Media Research Centre

speed-driven fixes that serve populist political ends and industry interests at the expense of fundamental digital rights and privacy.

Recommendation: Policymakers should redirect attention towards regulating the business models of digital platforms, not expanding them. Limiting data collection, ensuring transparency of algorithmic profiling and content moderation, and enforcing meaningful rights to data access and deletion are more effective strategies than mandating and encouraging new layers of surveillance.

c) the technical implementation and efficacy of age verification and content filtering mechanisms;

The technical implementation of age-verification and content-filtering mechanisms is fraught with challenges that were well known[12] in advance of the AATT trial, and which remain unresolved. The trial design appears calibrated to deliver a favourable verdict: it relied heavily on evaluation methodologies championed by technology vendors and industry evangelists, while taking little notice of the substantial academic and civil society evidence documenting bias and privacy risks. Few attempts seem to have been made to seriously contend with persistent issues of racial and gender bias, or to account for intersectional harms. As one former advisory board member, John Pane, Chair of Electronic Frontiers Australia, observed, the report was “strong on hype and rhetoric, and difficult to reconcile with the evidence”.

Despite the trial being framed as a success and selectively harvested for political talking points, a consistent finding is that many of the ‘best’ age-estimation technologies still have unacceptably high error rates, most notably for individuals close to the age cut-off (e.g. 16), for non-Caucasian users, for female-presenting persons, and for under-represented Indigenous communities.

The “grey zone” uncertainty near legal thresholds means the greater proportion of legitimate users risk wrongful exclusion at the thresholds of age verification. There is still little public accountability or clarity concerning how fallback or secondary verification mechanisms will work in practice, using the so-called “waterfall approach”. We fear that providers will simply seek compliance by forcing users to hand over increasingly sensitive personal documents and data. In any case, as predicted, the net effect is likely to create uneven burdens and exclusions for marginalised communities[13].

Claims from industry evangelists regarding future improvements to accuracy also fail to contend with the fact that determined young people can readily circumvent such systems through VPNs, borrowed devices, or alternative services[14]. Recent UK experience illustrates this vividly: BBC reporting[15], and similar studies[16], revealed how easily teenagers can bypass technical mechanisms to reach restricted content despite new rules.

---

[12] Stardust, Z., Obeid, A., McKee, A., & Angus, D. (2024). Mandatory age verification for pornography access: Why it can’t and won’t ‘save the children’. *Big Data & Society*, *11*(2). https://journals.sagepub.com/doi/10.1177/20539517241252129
[13] Ibid.
[14] Blake, P. (2018). Age Verification for Online Porn: More Harm Than Good? *Porn Studies* 6(2): 228-237. https://www.tandfonline.com/doi/full/10.1080/23268743.2018.1555054
[15] McMahon, L., Singleton, T., & Hayes, G. (2024, November 28). ‘It’s so easy to lie’: A fifth of children use fake age on social media. *BBC News.* https://www.bbc.com/news/articles/cn4v52ezx17o
[16] Unbelievably easy online age checks tricked in UK. (2025, July). *Information Age.* https://ia.acs.org.au/article/2025/unbelievably-easy-online-age-checks-tricked-in-uk.html

QUT Digital Media Research Centre

Enforcement efforts have triggered unintended effects as well. TechCrunch documented that VPN downloads surged after the UK's adult-content age-check rules came into force[17]. These examples show that while determined teenagers easily avoid verification, the young people most in need of supportive interventions, those without private devices or tech skills, are the ones most likely to be locked out, undermining the very purpose of the system.

Filtering technologies are no more reliable. False positives result in the blocking of legitimate educational or health content, including sexual health resources that young people urgently need. False negatives mean that harmful content slips through undetected. The technical promise of a perfect filter is illusory. More importantly, focusing on filters ignores the fact that children engage with online spaces for socialisation, creativity, and exploration. Attempting to sanitise or wall off these environments misunderstands their cultural importance.

Recommendation: Technical interventions for age-gating access to digital services should be recognised as blunt instruments, useful only in exceptionally limited circumstances. Policymakers must avoid overpromising on what technical filters can achieve. Resources would be better spent supporting the co-design of safe and positive online spaces with young people themselves.

d) alternative technical approaches to online safety for all users, including young people;

While technical measures are not sufficient, more proportionate and flexible approaches are available. For example, platforms can offer opt-in parental controls, default-on but customisable safety features, and transparent reporting tools. These allow families, and teens, to shape their own approaches to online safety, rather than imposing blanket restrictions that fail to account for diverse needs.

However, the real priority should be investment in long-term social interventions. International research demonstrates that **digital literacy programs in schools, libraries, and community groups are far more effective in building resilience than technical solutions.** In Finland, for example, media literacy education is integrated across the curriculum, contributing to high levels of resilience against misinformation and harmful content. Scandinavian countries have invested heavily in social support programs for children's digital lives, with significantly greater success than countries pursuing narrow technical controls. The effectiveness of such programs is evaluated through independent academic research[18], which allows for identification of further opportunities for enhancing the digital literacy of young people.

Evidence from Australia shows that young people are not passive victims online. Research from the University of Sydney found that 12–17 year-olds actively take charge of their online safety, are sophisticated platform users, and want a seat at the table in policy consultations[19]. Young people in Australia and globally actively utilise search engines and peer Q&A sites like Reddit to find answers to

---

[17] VPN downloads spike as UK introduces age checks for adult content online. (2025, July 28). *ITV News.* https://www.itv.com/news/2025-07-28/vpn-downloads-spike-as-uk-introduces-age-checks-for-adult-online-content

[18] Carlsson, H., & Sundin, O. (2020). Educating for Democracy? The Role of Media and Information Literacy Education for Pupils in Swedish Compulsory School. In A. Sundqvist, G. Berget, J. Nolin, & K. I. Skjerdingstad (Eds.), *Sustainable Digital Communities* (pp. 307–326). Springer International Publishing. https://doi.org/10.1007/978-3-030-43687-2_25

[19] Humphry, J., Boichak, O., & Hutchinson, J. (2023). Emerging online safety issues: co-creating social media with young people-research report.

QUT Digital Media Research Centre

questions around sexual and other health concerns[20]. From the perspective of young people, online access to such information is crucial as topics like health and sexuality tend to invite paternalistic and judgemental interactions offline[21].

Young people already have repertoires of digital safety skills, and their capabilities are growing[22]. They actively seek out informational resources on the topics of concern to the inquiry such as heath and sexuality. Research found that young people have the capacities to distinguish between low-quality and high-quality sources[23]. Policy should build on these strengths rather than assuming deficit and ensure the availability of high-quality online information on the topics relevant to young people. We note again the paradox that bespoke websites and other digital products created by leading scholars and policymakers to reliably inform youth may not reach these audiences due to overzealous filtering and blocking[24]. In addition to parents, teachers, and librarians, digital technologies like search engines act as such intermediaries[25]. It is crucial then that we independently evaluate how efforts to filter and block genuinely harmful content impacts the delivery of high-quality information that is relevant to young users and should be available to them.

Recommendation: The government should prioritise co-designed education programs and technologies that empower young people and the wider community. Instead of seeking to protect children *from* the digital environment, policy should focus on protecting them *within* it. This means investing in high-quality, free, age-appropriate digital products and services, co-created with young people, rather than relying on technical bans.

e) appropriate oversight mechanisms for online safety codes;

Oversight of online safety codes must be independent, transparent, and accountable. Industry self-regulation has repeatedly failed in this domain, with platforms setting standards that suit their commercial interests rather than the public good. The conduct of the AATT underscores these dangers: the oversight architecture was disregarded in practice, with advisory board members denied access to key findings and evidence. **Some vendors were reported to over-anticipate law-enforcement or coronial access to retained data, and to collect more data than necessary for age assurance, creating serious risks of privacy violations, mission creep, and misuse, particularly for adolescents and others with limited digital literacy.** Leaving code implementation and evaluation in the hands of industry-led bodies risks regulatory capture, mission creep, and weak enforcement.

---

[20] Gliniecka, M. (2024). *Youth digital health and online platforms: Dialogue with peers on Reddit*. Routledge.
[21] Healy-Cullen, S., Morison, T., Taylor, J. E., & Taylor, K. (2024). What does it mean to be 'porn literate': Perspectives of young people, parents and teachers in Aotearoa New Zealand. *Culture, Health & Sexuality*, *26*(2), 174–190. https://doi.org/10.1080/13691058.2023.2194355
[22] eSafety Commissioner, "The Digital Lives of Aussie Teens," eSafety research, February 2021, https://www.esafety.gov.au/research/digital-lives-of-aussie-teens.
[23] Cooper, S. C., Ferreira, K., Edwards, R. G., Keegan, J., Norvila, N., Lewis, L., Albury, K., & Skinner, S. R. (2024). A Qualitative Exploration of Young Australians' Lived Experiences of Social Media Use and Sexual Agency. *Sexuality & Culture*, *28*(2), 534–553. https://doi.org/10.1007/s12119-023-10131-w
[24] Turvey, J., Raggatt, M., Wright, C. J. C., Davis, A. C., Temple-Smith, M. J., & Lim, M. S. C. (2025). A Digital Pornography Education Prototype Co-Designed With Young People: Formative Evaluation. *JMIR Formative Research*, *9*(1), e65859. https://doi.org/10.2196/65859
[25] Nagappa, A., & Zendel, O. (2025, July 17). *What is Search Experience?* Automated Decision-Making and Society. https://medium.com/automated-decision-making-and-society/what-is-search-experience-39a3444bf1cd

A sustainable oversight model should be multi-stakeholder, drawing on the expertise of independent academics, civil society organisations, educators, child welfare experts, and privacy advocates. Oversight should not be dominated by industry actors or confined to centralised government agencies alone. Effective accountability requires distributed models of evaluation and consultation, rooted in community needs and local contexts.

Crucially, oversight must shift away from purely technical box-ticking (whether age verification has been deployed, or whether filtering tools exist) and instead ask whether interventions are improving outcomes for children and young people. This demands long-term investment in independent, public-interest research with guaranteed access to platform data. Without such evidence, regulation risks becoming performative rather than effective. **At present we still have no public independent evaluative framework to track the success or failure of one of the most dramatic interventions in our modern media landscape.**

Australia should also move beyond the idea that online safety can be achieved through national-level solutions alone. Community-led approaches, developed in partnership with young people and those who support them—families, schools, libraries, and local organisations—are essential and superior. These approaches are better placed to respond to the diverse cultural and social realities of digital life, and avoid the bluntness of one-size-fits-all national policy.

Recommendation: Establish an oversight framework that centres independent, academic, and community-based expertise rather than expanding government or industry control. This should include resourcing independent researchers with access to platform data, embedding civil society voices in decision-making, and supporting community-led digital literacy and safety programs as part of ongoing evaluation. Oversight should be judged by outcomes in practice, not the mere existence of technical compliance mechanisms.

f) global experience and best practice;

International evidence underscores that technically-driven online safety measures, particularly mandatory age verification, often fail in practice and carry serious unintended consequences. The United Kingdom's recent introduction of mandatory age checks under the Online Safety Act has already led to swift backlash and practical problems. Platforms including Reddit, X (formerly Twitter), Spotify, and even Wikipedia have been drawn into the scope of the law, required to adopt intrusive forms of verification such as photo ID, facial scans, credit card checks, or mobile verification. Almost immediately, users turned to VPNs to bypass the measures. As mentioned earlier, Proton VPN reported a 1,400 percent surge in sign-ups in the UK and VPN apps quickly became the most downloaded free tools in the Apple app store[26]. Analysts noted that these spikes reflected a lack of trust in intrusive systems and warned that safety cannot come at the expense of autonomy and privacy.

Public resistance has also been significant. An online petition to repeal the UK's Online Safety Act has gained over 500,000 signatures[27], while digital rights groups warn that the system introduces fresh risks of data breaches, censorship, and encroachment on encryption and anonymity. Smaller

[26] Smith, J. (2025, July 29). Proton VPN UK age-verification signups surge. *Mashable.* https://mashable.com/article/proton-vpn-uk-age-verification-signups
[27] https://petition.parliament.uk/petitions/722903

platforms and non-commercial services have also been caught in the net, including Wikipedia, which has challenged being subject to the same compliance burdens as large commercial platforms. As noted in response to (a), this experience highlights the dangers of rushing into technologically unworkable regulation that can be circumvented with ease, provokes public backlash, and disproportionately burdens smaller or public-interest providers.

By contrast, countries such as Finland, Sweden, and Indonesia have prioritised digital literacy and civic education as the cornerstone of online safety. Finland has embedded media literacy and digital citizenship across its school curriculum, with national agencies and independent organisations such as Faktabaari providing resources and training to support students, teachers, and communities. Indonesian media literacy organisation Mafindo, in addition to providing digital literacy training to first-time voters, high-school teachers, and seniors, provides free digital literacy modules for high school students, recognising that critical thinking and digital literacy skills are important sites of development for young people as well as a lifelong skill for all current and future users of digital systems. This whole-of-society approach is internationally recognised for building resilience against misinformation and harmful online content. These strategies work not by seeking to eliminate risk entirely, which is impossible, but by equipping young people with the skills and confidence to navigate complex digital environments safely.

The lesson is clear: Social interventions are durable and effective, while technical quick fixes are brittle and counterproductive. Australia risks repeating the mistakes of others if it invests heavily in technical solutions that cannot deliver on their promises. The evidence from overseas shows that investment in education, civic engagement, and community-led digital inclusion provides far greater and more lasting protection for young people.

Recommendation: Australia should position itself as a leader in evidence-based, socially grounded online safety policy. By learning from the failures of purely technical approaches overseas and aligning with global best practice in education and civic engagement, we can deliver outcomes that are both effective and respectful of rights.

g) any other related matters.

At its heart, this inquiry is about how Australia wants to approach the digital society. If we focus on a deficit model, with a reliance on banning and filtering, we will create a brittle system prone to failure, while deepening young people's distrust of institutions, and further entrenching platform power. If, instead, we invest in cultural, educational, and social strategies, we can build resilience that outlasts any specific platform or technology.

Young people are not simply to be shielded from the Internet. They are already active participants in digital culture and must be treated as partners in designing solutions[28]. International experience is already revealing how age bans are proving to be limited in achieving their intended objectives and, in some cases, have produced adverse psychological effects on adolescents[29]. **Excluding young**

[28] Humphry, J., Boichak, O., & Hutchinson, J. (2023). *Emerging online safety issues – Co-creating social media with young people – Research report*. The University of Sydney. https://hdl.handle.net/2123/31689
[29] McAlister, K. L., Beatty, C. C., Smith-Caswell, J. E., Yourell, J. L., & Huberty, J. L. (2024). Social Media Use in Adolescents: Bans, Benefits, and Emotion Regulation Behaviors. *JMIR mental health*, 11, e64626. https://doi.org/10.2196/64626

Australians through blunt technical tools risks driving them towards less visible, more harmful spaces. Empowering them, by contrast, builds the skills and confidence they need to navigate digital life.

Australia must also consider its broader human rights obligations. Children have a fundamental right to participate in digital society[30], to access information, and to enjoy opportunities for expression and association. Regulation that treats them primarily as potential victims rather than active citizens risks undermining these rights. There is no single "right age" for digital participation[31]; children's needs and capacities evolve, requiring tailored supports and tools rather than a blunt, one-size-fits-all cutoff. Selecting an arbitrary legal age for access ignores best evidence on how to foster healthy digital engagement and can inadvertently restrict the very opportunities that help children develop resilience and agency.

Recommendation: The Committee should explicitly recognise that online safety is not just a technical problem. It is a civic challenge requiring investment in people, not only infrastructure. Australia can lead by example, choosing education and empowerment over surveillance and exclusion.

[30] Livingstone, S., & Third, A. (2017). Children and young people's rights in the digital age: An emerging agenda. *New media & society*, *19*(5), 657-670. https://journals.sagepub.com/doi/abs/10.1177/1461444816686318
[31] Livingstone, S., & Sylwander, K. R. (2025). There is no right age! The search for age-appropriate ways to support children's digital lives and rights. *Journal of Children and Media*, 19(1), 6–12. https://doi.org/10.1080/17482798.2024.2435015

Digital Media Research Centre

Contributor Biographies

Professor Daniel Angus FQA

Daniel Angus is Professor of Digital Communication in the School of Communication, and Director of QUT's Digital Media Research Centre. His research spans computational communication, digital media, and public interest technology, with a focus on platform governance, algorithmic systems, and online discourse. He is a Chief Investigator and Chair of Infrastructure in the ARC Centre of Excellence for Automated Decision Making & Society (ADM+S), and a founding member of the Australian Internet Observatory, a nationally co-funded research infrastructure tracking digital media ecosystems.

In addition to his academic leadership, Daniel is a member of the Social Science Reference Group within the Office of the Queensland Chief Scientist, where he contributes to evidence-based policy and science communication strategies. His work is widely published across communication, media, and computational journals, and he is recognised for advancing interdisciplinary approaches to the study of digital platforms and their societal impacts.

Professor Axel Bruns FAHA FQA

Axel Bruns is an Australian Laureate Fellow and Professor in the Digital Media Research Centre and is a Chief Investigator in the ARC Centre of Excellence for Automated Decision-Making and Society. His books include *Are Filter Bubbles Real?* (2019) and *Gatewatching and News Curation: Journalism, Social Media, and the Public Sphere* (2018), and the edited collections *Digitizing Democracy* (2019), the *Routledge Companion to Social Media and Politics* (2016), and *Twitter and Society* (2014). He is one of the world's most cited social media researchers.

His current research focusses on the study of public communication in digital and social media environments, with particular attention to the dynamics of polarisation, partisanship, and problematic information, and their implications for our understanding of the contemporary public sphere; his work draws especially on innovative new methods for analysing 'big social data'. He served as President of the Association of Internet Researchers in 2017–19, and is an elected Fellow of the Australian Academy of the Humanities.

Dr Ashwin Nagappa

Ashwin Nagappa is a Post Doctoral Research Fellow at the QUT node of ARC Centre of Excellence for Automated Decision-Making and Society (ADM+S) and the QUT Digital Media Research Centre (DMRC). He is a recipient of the 2024 AXA Post-Doctoral Fellowship (for the theme 'Navigating misinformation and trust erosion in the digital age'). His research centres on emerging decentralized social media platforms, analyzing how they mitigate online harm and address challenges such as misinformation, hate speech, and polarization. Ashwin is also a research fellow in the Australian Search Experience 2.0 project, where he examines how search engines influence everyday data practices and knowledge sharing, particularly in relation to upholding public interest values like diversity and social cohesion.

Kateryna Kasianenko

Kateryna Kasianenko is a Research Fellow at the QUT node of ARC Centre of Excellence for Automated Decision-Making and Society (ADM+S) and the QUT Digital Media Research Centre (DMRC). Her PhD research focussed on practices of online engagement with Russia's war on

Ukraine in Japan and globally. Currently, she is examining how search practices and search interfaces shape each other and relate to real-world events, such as wars and crises, as well as social phenomena like partisanship.

Ned Watt

Ned Watt is a PhD candidate at the Digital Media Research Centre and the Australian Centre of Excellence for Automated Decision-Making and Society (ADM+S). Ned's doctoral research project, titled Generating Truths: Exploring the Intersection of Generative AI and Independent Fact Checking, examines how independent fact checkers respond to changes to the global communication environment brought about by generative artificial intelligence technologies. Ned's research examines how platforms and civic organisations respond to harms from online content and behaviour, including AI-generated content, highlighting where these efforts can be ineffective or even counterproductive.

Carly Lubicz-Zaorski

Carly Lubicz is a PhD Candidate at the Digital Media Research Centre. Carly has a professional background in media, communications, public affairs, and policy. Her research uses mixed method approaches, including social network analysis, to examine how information is being furthered in contemporary online communications spaces and how these dynamics could influence public support for policy.

Lucinda Nelson

Lucinda Nelson is a PhD candidate at the Digital Media Research Centre and the Australian Research Council Centre of Excellence for Automated Decision-Making and Society. She works at the intersection of regulation, media, technology, and violence against women. Lucinda's doctoral research examines the role of social media platforms in the manifestation and spread of everyday online misogyny.

Maria Margarita Ochoa-Diaz

M. Margarita Ochoa-Diaz is a PhD Candidate at the Digital Media Research Centre and is affiliated with the School of Teacher Education and Leadership. Margarita has an academic background in social science and cultural education, as well as youth-led digital peacebuilding. In her research, Margarita uses computational and qualitative methods to study youth's use of social media like TikTok and Instagram for political participation and peacebuilding. Her current research studies young political influencers' peacebuilding practices in post-conflict Colombia.

Dr Kim Osman

Kim Osman researches digital inclusion issues that impact the quarter of Australia's population unable to access and use digital technologies in the ways they want and need. Kim's research has enabled organisations and government to develop evidence-based policy and programs through her development of best-practice advice, guides, and toolkits for improving digital inclusion. Using place-based and ethnographic methods, Kim researches how social infrastructure like libraries support people to develop the digital skills and literacy needed to access education opportunities and fully participate economically, socially, and culturally in Australian society. Kim is a Senior Research Associate with the Digital Media Research Centre at the Queensland University of Technology.

Digital Media Research Centre

Associate Professor Michelle Riedlinger

Michelle Riedlinger joined QUT's School of Communication in July 2020. Her research interests include the emerging environmental, agricultural and health research communication practices, roles for "alternative" science communicators, online fact checking and public engagement with science. Her research is informed by theories of media, cultural approaches to science, social identity, and pragmatic linguistics. She coordinates QUT's Global Engagement Theme in the Global Journalism Innovation Lab and she has been a co-investigator on Social Sciences and Humanities Research Council (SSHRC)-funded projects investigating the online circulation of health research and online explanatory journalism. As a communication consultant, she has worked on projects focussed on climate variability, dryland salinity, ecology, catchment management, and river health. She has facilitated over two hundred communication training workshops for researchers. Michelle is the Editor-in-Chief of the Journal of Science Communication (JCOM). She is a member of the Scientific Committee of the Public Communication of Science and Technology Global Network, and she chairs the Finance Sub-Committee.

Professor Michael Dezuanni

Professor Michael Dezuanni undertakes research about digital media, literacies and learning in home, school and community contexts. He is the Program Leader for Digital Inclusion and Participation for QUT's Digital Media Research Centre which produces world-leading research for a creative, inclusive and fair digital media environment. He is also a chief investigator in the ARC Centre of Excellence for the Digital Child. Michael has been a chief investigator on six ARC Linkage projects with a focus on digital literacy and learning at school, the use of digital games in the classroom, digital inclusion in regional and rural Australia and in low income families, and the use of screen content in formal and informal learning. Michael is the author of 'Peer Pedagogies on Digital Platforms - Learning with Minecraft Let's Play videos' (MIT Press 2020), he has edited three academic books, and is the author of over 45 journal articles and book chapters. Michael has served on advisory committees for the Australian Digital Inclusion Alliance, the Australian Media Literacy Alliance, national charity The Smith Family, the Australian Curriculum and Assessment Authority (ACARA), the Alannah and Madeline Foundation, and Facebook Asia Pacific.

Dr Zahra Stardust

Zahra Stardust is a porn studies scholar interested in the regulation of sexual cultures. Her work specialises in sexual media and sextech, focusing on the politics of sexual content moderation (including the production, distribution and regulation of explicit media), and the development of community-led, social justice sextech. Her first book Indie Porn: Revolution, Regulation and Resistance (Duke University Press, 2024) explores the clash between indie porn producers, governments and big tech. Her next co-authored book, Sextech: A Critical Introduction (Polity Press, 2025), explores key debates in sextech design, manufacture and governance. Zahra is a Lecturer in Digital Communication at the Queensland University of Technology, a Chief Investigator in the Digital Media Research Centre, and an Affiliate at the Berkman Klein Centre for Internet and Society at Harvard University.

Dr Sebastian Svegaard

Sebastian Svegaard is a Postdoctoral Research Associate in the Digital Media Research Centre. His work sits within the ARC Laureate Fellowship project Determining the Drivers and Dynamics of Partisanship and Polarisation in Online Public Debate. Currently, he investigates discursive practices

in Australian and British news video content, as well as political leaders' use of social media during election campaigns. Sebastian uses a wide range of interdisciplinary approaches and focuses on cross-cultural comparisons within his work. His background is in media and cultural studies, particularly within the audio-visual media space.

Dr Samantha Vilkins

Samantha Vilkins is a Postdoctoral Research Associate in the Digital Media Research Centre, working on the ARC Laureate Fellowship project Determining the Drivers and Dynamics of Partisanship and Polarisation in Online Public Debate. Her background is in mathematics and science communication, and her PhD was in the role of interpretation in producing and communicating statistics in public discourses. She has drawn on her expertise and experience from both academic research and professional roles in communication and design in consulting for government as well as national associations and related stakeholders, including the Department of Agriculture, the Department of Foreign Affairs and Trade, Science Technology Australia, the Australian Academy of Science, and the Australian Council of Learned Academies.

Katherine M. FitzGerald

Katherine FitzGerald is a PhD Candidate at the Digital Media Research Centre. Katherine has an academic background in psychology and digital communications. Katherine has published in journals such as the *Harvard Kennedy School Misinformation Review*, *Media International Australia*, and contributed her expertise to multiple edited volumes. She uses qualitative and digital ethnography methods to study conspiracy theories, information disorder, and knowledge production on digital platforms.

Digital Media
Research Centre

About the Digital Media Research Centre

The QUT Digital Media Research Centre (DMRC) conducts world-leading communication, media, and law research for a flourishing digital society. Established in 2015, it is one of the top Australian centres for media and communication research, areas in which QUT has achieved the highest possible rankings in the national research quality assessment exercise ERA, and it is closely linked with the QUT School of Communication.

The Centre incorporates the QUT node of the Australian Research Council (ARC) Centre of Excellence for Automated Decision-Making & Society (ADM+S), and more recently the GenAI Lab. The Centre also participates in the ARC Centre of Excellence for the Digital Child, headquartered in the Faculty of Creative Industries, Education and Social Justice. QUT, through the DMRC, is also a founding member of the Australian Media Literacy Alliance. Its current Chair is DMRC program leader Professor Michael Dezuanni.

The DMRC works across four programs, which include:

Transforming Media Industries & Cultures
Digital Publics
Computational Communication & Culture
Creating Better Digital Futures

The Centre draws together leading researchers from six Schools and three Faculties, to investigates the digital transformation of the media industries, the challenges of digital inclusion and governance, the growing role of AI and automation in the information environment, and the role of social media in political polarisation. The DMRC has an international reputation for both critical and computational methods, and has access to cutting-edge research infrastructure and capabilities in areas such as social media analytics and critical simulation.

We actively engage with industry and international partners in Australia, Europe, Asia, the US, and South America; and we are especially proud of the dynamic and supportive research training environment we provide to our many local and international graduate students.

The DMRC is also a member of the global Network of Centres – a group of academic institutions with a focus on interdisciplinary research on the development, social impact, policy implications, and legal concerning the Internet.

We address local, national and global challenges at the forefront of digital transformation, and provide an ambitious, stimulating and supportive research culture for our researchers, students, and partners.

For further information, see: http://research.qut.edu.au/dmrc