2025 Australian Internet Governance Forum

Insights Report

April 2026

.au Domain Administration Ltd

Table of contents

About this insights report

This report has been prepared by auDA to draw out action-relevant insights from the 2025 Australian Internet Governance Forum (auIGF). The insights are based on ideas for considerations raised during the discussion and the report is intended to collate these suggestions. They are not recommendations by auDA.

The auIGF is an annual event for the discussion of public policy issues relating to the internet in Australia. It brings together a multidisciplinary community committed to deepening understanding of internet-related issues and the diverse perspectives of stakeholders across government, industry, civil society, academia and the technical community. auIGF provides an inclusive platform to explore Australian technology policy challenges, mobilise collaboration on solutions, and connect Australia to the regional and global Internet Governance Forum community. auIGF 2025 had more than 200 attendees, in person and online.

The aim of this report is to provide concise insights. We hope Australian decision-makers will use the accessible and actionable insights arising from the auIGF's proceedings to inform their future work.

For each session we set out a brief summary, followed by some key takeaways for Australia. We then set out matters for the future consideration of industry, auDA and Australian governments. The ideas presented are for parties to consider through their usual processes – their inclusion in this paper is not auDA committing to pursue them, nor is it a specific request from auDA for other parties to commit to them.

This paper is derived from the discussions at the Forum, as captured in the published auIGF 2025 Session Report and the event transcripts. References to legislation, reviews and policy processes have been added only where they help explain the current Australian policy context.

Should you wish to discuss or provide feedback on this report, please contact the team at internet.governance@auda.org.au.

Note: The content of this report is based on contributions and perspectives of panellists and participants shared during the public sessions of the auIGF. Following each session summary, it sets out auDA's understanding of the information shared and suggests matters arising that stakeholders could consider. The summaries were generated using external AI tools (ChatGPT) and have not been checked with the speakers, and so auDA does not assert that the report necessarily represents the views, positions or policies of the participants.

Session 1: Opening plenary

The opening plenary combined a keynote on global internet governance by Chris Buckridge (internet governance consultant) and a panel on Australia's digital governance trajectory. There was broad support for multi-stakeholder approaches and for strengthening domestic capability, so Australia is not overly reliant on external expertise or imported policy frames. The session noted a lack of a comprehensive national plan for Internet governance across all stakeholder groups and discussed whether the proposed *Social Contract for Digital Wellbeing* could provide the foundations for such a vision. The importance of diverse stakeholders coming together to analyse all facets of contemporary policy issues, and providing these insights to decision-makers, was a recurring theme.

Key takeaways for Australia

For Australia, the common themes were the need for stronger domestic capability, upholding internet governance as a multi-stakeholder system that can protect the internet's evolution, and how the auIGF can sharpen its focus on highlighting all aspects of an issue - and the tensions between different interests - to help better inform policymakers.

For further consideration

By industry

- Participate in and support multi-stakeholder approaches to internet governance and digital policy, to help ensure that policy develops in ways that are stable and well-thought through
- Contribute resources to capacity building in internet governance and digital policy, especially for civil society and user voices, to reinforce the capability and legitimacy of this approach

By government

- Use multi-stakeholder frameworks to resolve challenging policy problems where this is feasible, encouraging diverse stakeholders to generate consensus and workable outcomes
- Ask dialogue forums like auIGF to consider specific policy challenges, to tease out tensions and widen the analysis of difficult policy issues, potentially generating novel solutions
- Continue participating effectively and consistently at events like auIGF, the Pacific Islands Internet Governance Forum (Pacific IGF) and the Asia Pacific Regional Internet Governance Forum (APrIGF). Governments are a vital participant in these forums, and their presence encourages other stakeholders to participate, leading to a stronger internet governance system. They also provide an opportunity for governments to learn more about the concerns and opportunities other stakeholders are facing, leading to stronger policy locally.
- Make resources available to support under-represented stakeholders to participate in multi-stakeholder processes.

By auDA

- Strengthen the work of multi-stakeholder internet governance forums, by focusing on improved inclusion of under-represented stakeholders and on new working methods that support stronger policy outcomes
- Support the sharpening of work and post-event reporting in auIGF to better tease out policy tensions and alternatives, and propose recommendations for the multi-stakeholder community to consider, so that the dialogue is more useful in shaping real-world policy outcomes.

Session 2: The Commonwealth in conversation: World Summit on the Information Society 20-year review (WSIS+20) Reflections

This fireside chat between William Lee (Australian Government negotiator in the WSIS+20 review) and Cheryl Langdon-Orr (Internet Australia) explained the purpose of the WSIS+20 review and issues canvassed in the review. Some of the underlying tensions in the WSIS framework (e.g. between countries supporting multi-stakeholder internet governance, and those seeking a more intergovernmental approach) were explored. The goal was to explain to the auIGF community what the Review is considering and the issues at stake.

Key takeaways for Australia

The WSIS framework represents international endorsement of Australia's preferred multi-stakeholder approach to internet governance. It is also the framework that sustains the global Internet Governance Forum (IGF) (the UN General Assembly resolution A/RES/80/173 resolved to make the IGF permanent). It is in Australia's interests to maintain this framework and to support its ongoing evolution to strengthen the WSIS vision.

For further consideration

By industry

- Support the IGF and other relevant WSIS processes through participation, ideas for improved effectiveness, and contributions to the IGF itself, including ideas to reduce participation barriers.

By government

- Maintain international efforts to sustain multi-stakeholder internet governance
- Once the WSIS+20 review is concluded, continue to participate in shaping the WSIS framework
- Support the IGF, including by considering financial contributions to its Secretariat, and supporting broader Australian participation in the IGF
- Contribute to WSIS Action Lines implementation, particularly by support for Pacific partners in this area.

By auDA

- Engage with the now-permanent IGF to shape its working methods to drive more implementable outcomes
- Make a financial contribution to the work of the IGF Secretariat and encourage other country code Top Level Domains (ccTLDs) to do the same
- Consider options before the next IGF cycle to support broader Australian community participation in the IGF framework (nationally, regionally and globally) through a participation fellowship program.

Session 3: No-one left behind - digital inclusion and AI equity

The session treated digital inclusion as foundational to social and economic participation and argued that AI makes the issue more urgent. There was little disagreement about the need for action, but strong emphasis that action cannot be one-size-fits-all. Participants pointed to different barriers across affordability, accessibility, device access, skills, confidence, safety and service design, and stressed that policy needs to be evidence-based and co-designed with affected communities.

Key takeaways for Australia

Around one in four Australians are digitally excluded. This creates a social equity challenge and limits productivity and innovation as services increasingly rely on digital and AI systems. To maximise the potential of the modern technology environment, driving improved digital inclusion is essential.
Relevant context includes Closing the Gap Target 17, the First Nations Digital Inclusion Plan 2023-26 and Roadmap, and state initiatives such as the NSW Digital Inclusion Strategy.

For further consideration

By industry

- Design accessible, inclusive digital products and services, including for mobile-first and low-connectivity users
- Invest in digital literacy and confidence-building, especially for disadvantaged communities
- Support flexible skills frameworks for people and institutions building digital capability that evolve with technology
- Collaborate with government, civil society and community organisations to ensure products and services reflect the practical needs of users, including affordability, access to devices and connectivity, digital literacy, accessibility requirements, and safe and culturally appropriate service design.

By government

- Make digital inclusion a core, whole-of-government policy priority
- Early action areas could include:
    - A national device bank
    - Measures to improve the affordability of broadband services
    - Further promoting digital literacy and critical thinking in schools
- Encourage policy development in this area to be evidence-based, co-designed and human-centred, using multi-stakeholder approaches - as not all communities share the same challenges or needs
- Develop a common national digital skills framework, from pre-foundational to advanced, to support workforce and lifelong learning pathways

By auDA

- Articulate the need to embed digital inclusion in internet policy to help keep Australia's digital ecosystem open, trusted and inclusive.

Session 4: Digital platform ownership – diversity, resilience and trust

The session highlighted the lack of competition in Australia's network media economy. Speakers broadly agreed that Australia's network media economy is highly concentrated and that over-centralisation creates both technical and social risk, and geopolitical tensions are contributing to a growing "splinternet" at a governance level - fragmenting the internet into different regulatory and governance models. The discussion also distinguished between trust at the technical layer, where the internet often appears reliable, and trust at the governance and human layers, where transparency, accountability and care for users are more contested. Speakers highlighted that a diverse and distributed internet is essential to resilience and trust, reducing the risks of single points of failure from both technical outages and social harms such as censorship.

Key takeaways for Australia

- Australia's digital ecosystem is highly concentrated, with core internet services dominated by a small number of platforms, increasing national risk when systems fail or trust is lost
- A diverse and distributed internet is critical to Australia's democratic, cultural and economic outcomes and to reducing single points of failure, both technical (outages) and social (censorship or platform collapse)
- The rise of the "splinternet" increases complexity and risk for Australia as a globally connected, trade-exposed economy and should be minimised where possible
- Trust is fragile at the governance and human level and depends on competence, transparency and care; it is easily undermined by data breaches, misinformation and poor platform practices
- While permissionless innovation allows alternatives to emerge, Australia faces practical resilience gaps. These include limited prevention funding, poor supply-chain visibility, skills shortages, and weak coordination between policymakers and technical operators.
- Relevant policy context includes the ACCC's Digital Platform Services Inquiry final report.

For further consideration

By industry

- Reduce reliance on single, dominant platforms by using more diverse and distributed systems
- Invest in prevention and resilience, including redundancy, planning and regular stress-testing, rather than only responding after failures occur
- Map digital supply chains to identify hidden dependencies and enable risks to be managed more effectively
- Strengthen trust through better security, greater transparency, and clear care for users and communities
- Build workforce capability by investing in formal skills development and training to manage large-scale digital systems and incidents.

By government

- Reduce risk by encouraging more competition, diversity and decentralisation in digital infrastructure and Australia's network and media economy (i.e. telecommunications, traditional media and the digital platform economy) to avoid single points of failure
- Plan ahead and encourage preventative measures (e.g.: skills development, supply-chain visibility, risk planning) through regulation and investment not just crisis response
- Strengthen trust building governance, including transparency, accountability and user protection
- Improve coordination and policy alignment between government, regulators and technical operators.

By auDA

- Promote best practice in domain security, including uptake of domain name system security extensions (DNSSEC) and other protective measures, across the Australian domain ecosystem
- Support research and data-sharing on domain name system (DNS) usage, threats and trends to improve evidence-based policy development.

Session 5: Multi-stakeholder ways to improve trust in Australia's digital ecosystem

The panel agreed that trust in communications services has been strained by outages, rising expectations and poor communication when things go wrong. They could not agree on the right regulatory response. One view was that the Telecommunications Consumer Protections Code and current co-regulatory arrangements are no longer fit for purpose. Another was that direct regulation is not a cure-all, that the existing system is co-regulatory rather than purely self-regulatory, and that heavier compliance burdens can entrench larger providers at the expense of smaller ones. A third strand of discussion stressed that, whatever the model, trust depends on meaningful consultation, clearer accountability and more independent ways of resolving trade-offs.

Key takeaways for Australia

Communications networks underpin essential services, the economy, and public safety, so declining trust has nationwide social and economic consequences. Declining trust directly affects industry through reduced consumer confidence, higher regulatory scrutiny, and increased operational risk, particularly for smaller providers. The policy challenge is to improve reliability, transparency and accountability without assuming that either industry-led codes or direct regulation will, by themselves, resolve every trust problem. Relevant context includes the Telecommunications Consumer Protections (TCP) Code, related Australian Communications and Media Authority (ACMA) standards, and ACMA's October 2025 decision not to register the revised TCP Code.

For further consideration

By industry

- Industry and regulators should strengthen co-regulatory frameworks, clarify accountability and decision-making roles, improve outage communications, and embed resilience and reliability expectations in codes and regulatory settings.

By government

- Review and strengthen regulatory and co-regulatory frameworks to ensure they remain fit for purpose
- Clarify accountability and escalation arrangements between industry, regulators, and government
- Set clear expectations for transparency, reliability, and resilience in regulatory instruments
- Ensure regulatory settings balance consumer protection, competition, and impacts on smaller providers.

By auDA

- Trust and resilience in the digital ecosystem directly affect confidence in the .au domain, DNS stability, and Australia's online presence. This means auDA should continue to communicate its governance and policy settings for the .au domain to reinforce security, resilience, and trust.
- Support best practice standards and education that lift trust in Australia's digital infrastructure
- Commission research into trust - what it means and what factors drive improved public trust in the internet environment.

Session 6: New playgrounds, new rules: the future of child digital rights & skills

The session discussed how to protect children online while also supporting their digital skills development, drawing on recent policy debates in Australia, New Zealand and globally. Audience polling about the social media ban showed little confidence in social media bans and strong concern that young people are not well prepared for a digital and AI-driven future. Speakers agreed that online harms are real and that schools and communities need safer environments. However, views diverged on where responsibility should sit - across parents, schools, platforms, regulators and young people themselves - and on how much weight should be given to bans, age restrictions, community education and child participation in policy design. The need for community-based approaches that see digital tools as opportunities for learning, not just risks was emphasised.

Key takeaways for Australia

- Age restrictions alone are unlikely to meet policy goals to keep children safe online
- Participants emphasised that regulation may need to be complemented by platform design changes, education and community-based responses
- Preparing young Australians for a digital and AI-enabled future will require stronger digital, media and AI literacy, with schools, families and communities playing important roles in building these capabilities
- Responsibility for online safety is shared across parents, educators, platforms, regulators and young people themselves, suggesting that effective responses will require coordinated action across sectors
- These issues sit alongside the implementation of Australia's Online Safety Amendment (Social Media Minimum Age) Act 2024, which introduced a minimum social media age regime commencing on 10 December 2025.

For further consideration

By industry

- Embed child-centred, safety-by-design approaches rather than relying on bans or takedowns alone
- Build future talent pipelines by investing in digital and AI skills for youth to address risks of long terms skills and workforce shortages
- Strengthen trust and social licence through transparent practices and inclusive design (e.g.: transparent algorithms, age-appropriate design, and measurable harm-reduction outcome)
- Product and policy effectiveness can be improved by meaningfully including children and young people in design, testing, and governance processes.

By government

- Policy design should move beyond regulation-only responses and develop more balanced approaches to child online safety (e.g.: empowerment and digital skills development)
- Ensure future readiness by encouraging investment in digital and AI skills development to prepare young people for education and work
- Develop flexible and adaptive regulation to keep pace with rapid technological change
- Encourage and strengthen multi-stakeholder governance models, involving educators, families, industry, and civil society in policy design and implementation.

By auDA

- Issues of online safety and digital capability are central to trust in the online environment, aligning with auDA's stewardship of the .au domain.
- Promote safety-by-design and responsible online identity through domain name policies, registrar guidance, and best-practice resources.
- Position as a key convenor and steward, supporting cross-sector dialogue between government, industry, educators, and the technical community on child digital rights and online trust.

Session 7: How might approaches to digital inequities from the First Peoples of Australia and indigenous communities enhance global internet governance?

This session argued that digital inequity affecting First Peoples and Indigenous communities is not peripheral to internet governance but central to it. Speakers were aligned that top-down, standardised models can reproduce colonial harms through service design, infrastructure rollout, data practices and assumptions about inclusion. The sharper point of difference was conceptual: several speakers challenged whether inclusion is the right frame at all, arguing that equity, safety, self-determination and recognised Indigenous governance structures are more appropriate starting points.

Key takeaways for Australia

Aboriginal and Torres Strait Islander communities continue to face digital inequities in connectivity, affordability, literacy, and trust in digital systems. As Australia expands digital-first services and digital identity, there is a clear risk of exclusion by design. Embedding Aboriginal and Torres Strait Islander leadership, data sovereignty, and community-led infrastructure—while treating connectivity as essential—would support more equitable and resilient digital governance outcomes. Relevant context includes Closing the Gap Target 17, the First Nations Digital Inclusion Plan 2023-26 and Roadmap, and the growing importance of digital identity and digital-first service delivery.

For further consideration

By industry

- Design for equity and trust: embed Aboriginal and Torres Strait Islander perspectives in digital product and service design to avoid "exclusion by design" and build long term trust
- Partner early with communities and support community-led and community owned connectivity models. Community-led and Indigenous-owned models (e.g. Māori-run Internet Service Providers (ISPs) as seen in New Zealand) show that co-design and shared ownership can deliver more resilient, affordable and trusted connectivity outcomes than top-down approaches.
- Account for land, data and culture: Infrastructure, data and platform deployments should respect Aboriginal and Torres Strait Islander land rights, sovereignty and cultural knowledge, reducing reputational, operational and social risk
- Invest in affordable, resilient connectivity and local capability-building.

By government

- Embed Aboriginal and Torres Strait Islander leadership and decision-making in digital policy, service design, and governance
- Require co-design and consent for digital services and infrastructure, using early engagement and informed consent as a baseline
- Consider the design of digital-first services to avoid exclusion by design, ensuring offline alternatives, cultural safety, affordability, and low-connectivity access
- Treat connectivity as essential infrastructure by funding affordable, resilient access and supporting community-led and community owned models
- Fund and procure community-led and community owned models to support self-determination, trust, and long-term digital resilience.

By auDA

- Use auDA's convening power, grants and engagement programs to elevate Aboriginal and Torres Strait Islander voices and support community-led digital participation, safety and resilience.

Session 8: Fostering trust online for Australians – the human element

The session explored the tension between Australians' heavy reliance on the internet and relatively low trust in the online environment. There was broad agreement that cybercrime, misinformation and opaque data practices are major drivers of that gap, and that security should not rest on individuals alone. Speakers nonetheless framed the consequences differently. For some, declining trust and opting out of online activity is a warning sign that threatens participation and productivity; for others, opting out can also reflect legitimate user agency where trust has not been earned. Discussion also distinguished between strong appetite for AI reform and lower public understanding of newer systems such as Digital ID.

Key takeaways for Australia

For Australia, this discussion sits alongside current work on privacy reform, the Digital ID framework, the 2023-2030 Australian Cyber Security Strategy, and Australian Government guidance on AI safety and adoption. The policy gap identified in the session was not only one of law, but one of public understanding: there is appetite for stronger safeguards, but also low awareness of how newer systems such as Digital ID work and what protections already apply.
See auDA's *Digital Lives of Australians 2025* research report for more insights.

For further consideration

By industry
- Address falling trust in digital services which threatens customer uptake, innovation and industry reputation—especially for AI and digital identity
- Embed privacy-by-design and minimise and secure data collection
- Be transparent about how data and AI are used, including risks and safeguards
- Strengthen cyber security as a core business practice, not an add-on.

By government
- Strengthen privacy and data protection to limit data misuse and improve accountability
- Set clear safeguards and oversight for AI and Digital ID to build public trust
- Lift baseline cyber security standards across government and industry
- Improve public understanding through simple, consistent communication and guidance.

By auDA
- Provide practical guidance to help members adopt secure, transparent digital practices
- Act as trusted intermediary between industry, government and the community to build confidence in digital systems.

Session 9: Closing plenary

The closing plenary drew together reports from the sessions, an "open microphone", and a closing panel on what the Australian internet governance community should do next. There was broad support for the auIGF becoming more outcome-oriented and for continuing work on a *Social Contract for Digital Wellbeing*. This report is an example of a more outcome-oriented way of working.
At the same time, the closing discussion made clear that several questions remain open: how broad auIGF's scope should be, how it should relate to other government-led consultation processes, how far it should go in documenting disagreement as well as consensus, and how to widen participation without losing focus.

Key takeaways for Australia

Strengthening the national fabric of internet governance in Australia will increase its effective contribution to national policy debates and strengthen the ability of internet governance to shape the internet and its impact in a positive direction. Such strengthening is the domestic fulfilment of Australia's public international commitment to multi-stakeholder internet governance.

For further consideration

By industry
- Engage in the auIGF and be part of the dialogue to help inform other stakeholders' views about industry priorities and insights, and to learn from theirs
- Push for clear outcomes and sharing of insights from auIGF and other internet governance forums as a condition of support and participation.

By government
- Make use of the auIGF to tease out complex policy and governance problems related to the internet and digital technology
- Continue to support the auIGF as a process with relevant government departments, regulators and other agencies encouraged to participate

By auDA
- Continue to support the auIGF as Secretariat and improve its outputs, and work to support the auIGF to determine its program and approach as early as possible
- Advocate to the auIGF Multi-Stakeholder Steering Committee (MSSC) to:
    - Clarify the auIGF's scope and mandate, to make it more accessible. The scope should continue to extend past technical coordination and internet governance into wider digital policy matters
    - Deepen and diversify participation, especially by recruiting participants who need to be part of the conversation for specific sessions to generate well-rounded consideration
    - Share the outputs and insights from the auIGF into other relevant technical coordination, internet governance and digital policy processes
    - Continue to develop an environment where tensions and disagreements can be discussed openly and respectfully in ways that drive mutual understanding and dialogue around conflicting interests and policy outcomes.

Further information

auDA will publish a similar report after the 2026 auIGF.

You can find out more about the Australian Internet Governance Forum at their website. The site includes information about last year's event, the Position Paper process, and how to get involved. The 2026 auIGF will be hosted in Canberra in September – sign up on the website for news about the Forum.

Further information about auDA's internet governance and public policy work is also available. To get in touch with the team contact us at: internet.governance@auda.org.au.