Quarterly Public Policy Report

auDA's Public Policy Report - July to September 2023 (FYQ1)

Recap: What we got up to last quarter

We hosted the **Asia Pacific Regional Internet Governance Forum (APrIGF)** in Brisbane from 28-31 August 2023. Three other key events including Australia's national IGF (NetThing), the Pacific IGF (PACIGF) and the Asia Pacific regional Youth IGF (yIGF) took place alongside the APrIGF. More than 250 in-person and more than 1,000 Zoom connections from 68 countries participated.

Themes discussed included internet fragmentation, generative AI, data governance, cyber security, content moderation, misinformation, digital inclusion, digital rights and democracy, and digital sustainability. You can read more about the event on our auDA blog or watch session recordings. Session transcripts will soon be available.

We also launched our inaugural **Internet Governance Roadmap 2023-2025** (the Roadmap), in which we set out an analysis of current and upcoming challenges within the internet governance system. At the core of the Roadmap is our belief that the multi-stakeholder approach is vital to the effective operation of the internet governance system. The Roadmap proposes a series of actions to sustain and improve multi-stakeholder internet governance. Our goal is to ensure the internet remains open, free, secure, and global, so the its social and economic benefits can continue to be enjoyed.

In this edition we cover in brief:

Domestic public policy matters	Internet governance and global policy
• **Privacy** • **Cyber security** • **Digital identity** • **Digital technologies** • **auDA's tech policy radar**	• **Internet governance** ○ Global Digital Compact ○ Asia Pacific Top Level Domain Association • **Global policy** ○ Digital Markets Act (DMA) ○ Web 4.0 and virtual worlds

Domestic public policy matters

Below, we provide an overview of latest developments on relevant policy issues – and our analyses and responses to those. In our Public Policy Agenda 2023-2024, you can find out more about auDA's priority policy areas.

Privacy

Identity Verification Services Bill 2023

On 13 September, the *Identity Verification Services Bill 2023* (Cth)(the Bill) was introduced to federal Parliament. The aim of the bill is to ensure identity verification services are secure and protect the privacy of Australians.

If passed, the Bill seeks to help organisations using identity verification services to authenticate identity documents to verify a person's identity in a way that is secure and private by putting in place safeguards and security measures to protect Australians online, including:

- **Secure systems** in which information and communications must be encrypted and data breaches must be reported
- **Limits on access** so that industry and most government agencies can only access identity verification services for 1:1 matching for the purpose of verifying identity, with the consent of the individual
- **Strong privacy protections** including consent requirements, privacy impact assessments, complaint handling and transparency about how information will be collected, used and disclosed
- **Penalties** for government and industry organisations that do not comply with their obligations, including terminating access to identity verification services.

The measures intend to strike the right balance between achieving fast and convenient identity verification while maintaining strong standards of privacy and security.

auDA's contribution:

We monitor this matter closely and are assessing the Bill and its linkage to the *Digital ID Bill 2023 (Cth)* also before parliament (see section on Digital identity).

Government response to the Privacy Act Review Report

In late September, the Australian Government released its response to the Attorney-General's Department's Privacy Act Review Report (the Report) published in February 2023.

The Report contained 116 proposals to overhaul the *Privacy Act 1988* (Cth) (Privacy Act) to make it fit for the digital age. The Attorney General has agreed and committed the Government to act on 38 of the proposals, and to introduce a Bill to Parliament in 2024. Another 68 proposals are agreed to 'in principle', while 10 have been rejected.

Where the government has agreed 'in-principle', those proposals will be subject to further engagement and a comprehensive impact analysis to ensure the 'right balance' is struck. Those proposals include:

- Expanding the definitions of personal information and sensitive information
- Removing the small business exemption
- Reducing the data breach notification period to 72 hours
- Introducing new legislative provisions regarding the retention of personal information
- Introducing further controls and individual rights regarding access, correction and erasure
- Expanding regulation of direct marketing, targeting and trading in personal information.

auDA's contribution:

Earlier this year, we made a submission to the Report. Some of the key points we raised addressed the definition of personal and sensitive information, small business exemption removal, data breach notification period, and individuals' right to erasure of their personal data. Most of those points raised were agreed to in principle in the government's response and we look forward to engaging further with the Attorney-General's Department on those matters.

Cyber security

In September, Minister for Home Affairs and Cyber Security, Clare O'Neil announced the 2023-2030 National Cyber Security Strategy (the Strategy) will be released "before the end of the year". According to Minister O'Neil, the new Strategy is built around **six cyber shields**:

- The **first shield** focuses on creating "strong citizens and business" and help them understand how to protect themselves
- The **second shield** focuses on safe technology and ensuring that citizens and businesses are protected "with a layer of safe products"
- The **third shield** is "world-class threat sharing and threat blocking" so that by 2030 we envision a world where threat intelligence can be exchanged between government and business in real-time and threats are blocked before they can cause harm to Australians

- The **fourth shield** aims to protect critical infrastructure from attack, including assets operated by government
- The **fifth shield** seeks to ensure Australia has a "thriving cyber ecosystem", where cyber security is a desirable profession for young people
- The **sixth shield** involves ensuring "coordinated global action" through engagement with international partners.

As expressed by Minister O'Neil, the forthcoming Strategy will also be unique from those of the past in that it will use two-year horizons to help Australia reach the ambitious goal of becoming the most cyber secure nation by 2030.

auDA's contribution:

We made a submission to the Department's consultation on the 2023-2030 Australian National Cyber Security Strategy and continue to monitor policy discussion on cyber security.

By attending and facilitating cyber security related roundtables, events and discussion forums, we share our views with government, civil society and industry. auDA staff frequently meet with relevant government officials to discuss cyber security policy and regulation.

Digital identity

On 19 September, the Department of Finance launched a consultation on the Exposure Draft for the Digital ID Bill 2023 (the Digital ID Bill) and Accreditation Rules (Rules), an important milestone in advancing the Australian Digital Identity ecosystem.

The Digital ID Bill aims to strengthen privacy and security rules for Digital ID providers and expand the Australian Government Digital ID system (AGDIS) to include private sector organisations that choose to opt in to the AGDIS.

The proposed Rules accompanying the legislation also impose cyber security incident reporting obligations on Digital ID providers and services. Providers will also have to provide risk assessments to the government for the IT systems they use for Digital ID services.

Importantly, the Digital ID Bill does not regulate Digital ID services generally. Only accredited service providers can participate in the AGDIS. For Australians with accessibility requirements, the Rules require Digital ID services providers to meet standard accessibility and usability requirements.

The Government outlined a four-phase process for the Digital ID rollout, with **phase one** being establishing the ID in legislation that also provides for regulation and accreditation of public and private providers.

In the **second phase**, state and territory Digital IDs will be recognised for accessing Commonwealth government services. In **phase three**, myGovID will be recognised by the private sector. In **phase four**, the government will begin recognising private sector Digital IDs to access government services.

The Australian Competition and Consumer Commission will be tasked with regulating Digital ID, with the Information Commissioner covering all privacy-related aspects. The introduction of the final bill is expected by the end of the calendar year.

auDA's contribution:

auDA made a submission on the Digital ID Bill and Rules. Our submission will be uploaded on our submissions website once published by the Department. In the meantime, you can read more about our stance on digital identity in our domestic public policy agenda.

Digital technologies and platforms

Misinformation and disinformation

In June 2023, the Exposure Draft Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2023 (draft CMD Bill) was released for public consultation, which closed on 20 August 2023.

In brief, the draft CMD Bill would provide the Australian Communications and Media Authority (the ACMA), with new powers to combat online misinformation and disinformation. The proposed powers would enable the ACMA to:

- Gather information from, or require digital platform providers to keep records regarding misinformation and disinformation
- Publish information on its website relating to misinformation or disinformation regulation, measures to combat the issue, and the prevalence of such content
- Request the industry develop industry codes covering measures to combat misinformation and disinformation which would be registered and enforced by the ACMA
- Create and enforce misinformation standards where ACMA deems an industry code to be ineffective.

The ACMA will not have the power to request specific content or posts be removed from digital platform services.

Concerns about whether the draft CMD Bill strikes the right balance have been expressed by a range of stakeholders including legal experts such as the Victorian Bar Council and Law Council of Australia. The full extent of feedback about the Draft Bill is not yet known, as the submissions have not yet been published by the government.

Some of the key concerns raised by commentators include:

- Vague and broad definitions of "misinformation" and "disinformation"
- Overly broad categories of harm, including "harm to the health of Australians" and "harm to the Australian environment", and no guidance on how harm should be judged
- Definitions of excluded content, which is content protected from being labelled as misinformation or disinformation.

The practical impact of the draft CMD Bill will depend on the content of the misinformation codes/standards, once developed.

auDA's contribution:

We continue to monitor developments regarding the draft CMD Bill.

Online safety

On 8 September, Australia's eSafety Commissioner announced it will register an online safety code covering internet search engines. The code will come into effect six months following registration and brings the number of completed industry codes governing the digital industry to six.[1]

The strengthened Search Code will require search engines to take steps to reduce the risk that material like child abuse material is returned in search results. It also ensures that AI functionality integrated with the search engines are not used to generate "synthetic" versions of this material.

[1] In June, the eSafety Commissioner registered industry codes for five online industry sectors, namely Social Media Services, Internet Carriage Services, App Distribution Services, Hosting Services, and Equipment providers.

auDA's contribution:

auDA monitors the eSafety Commission's work. Online safety, content moderation and regulation does not fall within the scope of auDA's operations and responsibilities. We adopt a collaborative approach and will always respond to lawfully authorised requests relating to .au domain names, including those from the eSafety Commissioner.[2]

Artificial intelligence

In June/July 2023, the Department of Industry, Science and Resources consulted on Safe and responsible AI in Australia. The discussion paper focused on identifying potential regulatory gaps in the existing domestic governance landscape and possible additional AI governance mechanisms to support the development and adoption of AI. It noted that not all issues related to AI are intended to be considered in the consultation, including the implications of AI on labour markets, national security and intellectual property.

auDA's contribution:

In our submission, we set out the need for human-centricity, privacy principles for AI systems, and emphasise the need to assess cyber security implications of AI systems. .

auDA's tech policy radar

Some other public policy matters on our radar are:

- **Electronic Surveillance Reform**: The Attorney-General's Department is leading this reform work, with further proposals expected later this year.
- **Copyright enforcement review 2022-23**: Further consultations and/or the release of draft legislation is expected by the end of 2023.

Internet governance and global policy

Internet governance

The Global Digital Compact (GDC)

A Preparatory Ministerial Meeting for the Summit of the Future was held on 21 September during the United Nations General Assembly High-level Week. Member States agreed

[2] For more information, see How auDA responds to requests from law enforcement.

that the Summit will adopt a Pact for the Future, negotiated by governments. Digital cooperation will be one of the focus areas for the Pact, along with sustainable development; international peace and security; science, technology and innovation; youth and future generations; and transforming global governance. The GDC is expected to form an annex to the Pact.

auDA's contribution:

On the auDA blog you can find out more about our stance on the GDC.

Asia Pacific Top Level Domain (APTLD) Association

APTLD's 84th members meeting was held in Seoul, Korea on 19-20 September. A highlight of the meeting was a celebration of APTLD's 25th anniversary, and the holding of a High Level Meeting of Members. The day prior a statement was agreed on the importance of the Internet for All, and how country code Top Level Domain (ccTLD) managers (like auDA) can contribute to realising this goal. auDA staff presented on the future of ccTLDs, WHOIS accuracy, and Environmental, Social, Governance (ESG) matters. You can find more information about the meeting and the various topics discussed on the APTLD website and in the communique published in late September.

Global Policy: what's happening overseas?

Digital Markets Act (DMA): European Commission designates gatekeepers

On 6 September, the European Commission designated six "gatekeepers" under the Digital Markets Act for the first time: Alphabet, Amazon, Apple, ByteDance, Meta and Microsoft. The companies now have 6 months to comply with the full list of do's and don'ts under the DMA, offering more choice and more freedom to end users and business users of the gatekeepers' services.

The Commission will monitor the effective implementation of and compliance with these obligations. In case a gatekeeper does not comply with the obligations laid down by the DMA, the Commission can impose fines up to 10 per cent of the company's total worldwide turnover, which can go up to 20 per cent in case of repeated infringement.

In parallel, the Commission has opened four market investigations to further assess Microsoft's and Apple's submissions arguing that, despite meeting the thresholds, some of their core platform services do not qualify as gateways:

- Microsoft: Bing, Edge and Microsoft Advertising
- Apple: iMessage

Find out more: European Commission designates six gatekeepers

Web 4.0 and virtual worlds: European Commission publishes its strategy to lead on Web 4.0 and virtual worlds

On 11 July, the European Commission published a strategy on virtual worlds and Web 4.0. It outlines a plan for addressing the challenges and making use of the opportunities presented by virtual worlds and the next iteration of the internet, which is expected to be based on advanced AI, IoT, blockchain, and immersive technologies – amongst others.

According to the strategy, "drawing from the lessons of the current internet", the development of virtual worlds is likely to pose challenges to fundamental rights and objectives of "general public interest in a democratic society", such as data protection and privacy, disinformation, cybersecurity, and consumer protection.

The Commission aims for a Web 4.0 that is powered "by open and highly distributed technologies and standards that enable interoperability between platforms and networks". Concerning concrete actions planned in the foreseeable future, the Commission expects to develop a "virtual worlds toolbox" that includes the use of "trustworthy digital identity and digital wallet solutions", consumer protection, cyber security and intellectual property.

Additionally, the Commission pledges to support the "creation of a technical multi-stakeholder governance process to address essential aspects of virtual worlds and Web 4.0 that are beyond the remit of existing internet governance institutions" (from early 2024).

On 4 August, the European Parliament's Committee on the Internal Market and Consumer Protection (IMCO) issued a draft report on "virtual worlds – opportunities, risks and policy implications for the single market", recommending further improvement to address the lack of a "universally recognised or agreed definition" of virtual worlds of the strategy, and making "the debate over the need for the identification of users in virtual worlds" a priority area, especially for the purpose of identifying individuals by the competent authorities.

Find out more: An EU initiative on virtual worlds: a head start in the next technological transition

What we're reading

The following articles related to internet governance and digital economy policy and regulation caught our eye, and may be of interest for further reading:

Title: **The Times Stand Still: Internet Shutdowns, the Irony of the Multistakeholder Process and Realpolitik**

- **What's it about:** When governments restrict internet access, they make a statement about the interpretation and application of the foundational principles that guide the functioning of the internet. Governments use internet shutdowns as a control tool, much like how states use political or military power to establish dominance.
- **Why we are interested**: As we navigate this digital age, there is a pressing need to reaffirm the multi-stakeholder model's effectiveness and ensure it remains resilient against the shifting dynamics of realpolitik and international diplomacy.

Title: Traditional Domain Names, New Environments: Integrating into Blockchains and Beyond

- **What's it about**: The opinion piece suggests that by establishing responsible integration for DNS domain names into blockchain applications, the DNS community can work towards increasing DNS domain name utility and supporting new use cases.
- **Why we are interested**: Views on blockchain domain names are divided. Some dismiss them as 'just another' alternative naming system, while others consider them as promising decentralised alternative. We monitor such developments closely.

Title: The UN wants more multilateral regulation of the digital world. Democracies should be worried

- **What's it about**: The Policy Brief elaborates on the risk of the GDC to further centralise and consolidate technology and digital governance issues in the multilateral system.
- **Why we are interested**: We support the message this article convenes, which is to encourage the broader international community to avoid duplicating well-established multi-stakeholder processes and instead refocus efforts to improve these processes so that they can evolve as needed.

Q4 2023 events

Events

21-26 October 2023
ICANN78 Hamburg, Germany
ICANN78 will mark the organisation's 25th Annual General Meeting (see schedule).

14 November 2023
Centr (Council of European National Top-Level Domain Registries) hosts its Annual Centr Meeting on 14 November 2023. More information will be made available soon on Centr's website.

Webinars

Over the next months, auDA is scheduled to host a series of webinars on public policy matters, debriefs on key internet governance forums and our research projects. Keep track of our webinar and events schedule and register here.

Open consultations – have your say

Agency	Consultation	Submission due date
Department of Finance	Digital ID Accreditation Rules	31 October 2023
ACMA	Review of Australian satellite filing procedures	11 October 2023
Portfolio Committee No. 1 – Premier and Finance	Artificial intelligence (AI) in New South Wales	20 October 2023

Contact us via public.policy@auda.org.au for more information on our policy and advocacy initiatives and other related matters.