

Quarterly Public Policy Report

April to June 2023

Welcome to auDA’s inaugural Quarterly Public Policy Report. This edition covers April – June 2023. In this report we provide a brief update of regulatory developments relevant to the internet industry and its stakeholders, and a sneak peek into auDA’s policy position on such matters.

In this first edition we cover:

Domestic public policy matters	Internet governance and global policy
<ul style="list-style-type: none">• Privacy• Cyber security• Digital identity• Digital technologies• auDA’s tech policy radar	<ul style="list-style-type: none">• Internet governance<ul style="list-style-type: none">○ Global Digital Compact○ ICANN77○ Internet & Jurisdiction• Global policy<ul style="list-style-type: none">○ The European Union’s AI Act○ The European Union’s Cyber Resilience Act

This report is intended as a tool for readers – to use in their own work on internet policy and governance, and to understand auDA’s priority areas. We provide a high-level overview on key topics. Readers should do their own deeper research on topics they are interested in.

We encourage you to share your feedback about this report with us. You can email us at public.policy@auda.org.au.



Domestic public policy matters

It's been an interesting quarter in digital economy policy. Given various cyber breaches and the release of generative AI tools, it is unsurprising that privacy, cyber security, digital platforms and new digital technologies including AI, remain key policy issues on the Federal Government's agenda.

We monitor and respond to a range of policy consultations touching on these matters.¹ In our [Public Policy Agenda 2023-2024](#), you can find out more about auDA's priority policy areas and our stance on them.

Privacy

The Attorney-General's Department (AGD) is currently reviewing submissions on its [116 proposals for privacy law reform](#). The reforms expand the scope of what is protected under the Privacy Act. This could mean existing obligations apply in more circumstances, to more information and to processes that would not have previously been covered. Some of the proposed expansions are:

- **Personal Information** – The definition of personal information to be amended to include any information that *relates to* an individual (instead of information *'about an individual'*).
- **Sensitive Information** – The definition of sensitive information will be expanded to align with the expanded definition of personal information and to also include genomic information.
- **Automated Decision Making (ADM)** – The review proposes more transparency around personal information used in “substantially” automated decisions which have a legal or significantly similar effect on an individual's rights.
- **Small business exemption removal** – The proposed removal of the small business exemption could mean actively trading Australian small businesses that are presently outside the scope of the Privacy Act will be required to meet compliance obligations.
- **Notifiable Data Breach scheme** – The review proposes that the deadline for reporting eligible data breaches to the Office of the Australian Information Commissioner (OAIC) will be reduced to (a General Data Protection Regulation-

¹ Some of the policy matters are 'live' areas of policy debate in Australia. That means they are being assessed by the Federal Government on an 'ongoing' basis and do not necessarily fit neatly into one quarter, like the Digital Platforms inquiry 2020-2025 led by the Australian Consumer and Competition Commission (ACCC). We highlight those matters in the relevant sections.



familiar) 72 hours from when the entity becomes aware that there are reasonable grounds to believe that there has been an eligible data breach. Notification to impacted individuals must be completed 'as soon as practicable'.

auDA's contribution:

auDA has participated in privacy law reform debates since the AGD commenced its review in 2020. We have responded to public consultations and attended roundtables. [Our latest submission on the Privacy Act review](#) reiterates that we:

- Support privacy laws that better protect individuals and businesses
- Advocate for harmonisation with international privacy law
- Support the removal of the small business exemption after further provision of support to small businesses
- Support transparency of ADM systems and the right to subject automated decisions to review, preferably internal human review
- Support tighter timelines for breach reporting to better reflect community expectations and better protect Australians' data.

We will keep a close watch on this area and will provide further updates when additional details of reform proposals become available later this year.

Cyber security

The Government is taking steps to reform Australia's cyber security landscape. The development of the Department of Home Affairs' [2023–2030 Australian Cyber Security Strategy](#) (Cyber Security Strategy) comes at a pivotal time. While the discussion paper does not provide specific cyber security reform proposals, it invites comment on the state of cyber security and input on how to make Australia the most cyber-secure nation in the world. Key issues include:

- Enhancing cyber resilience across the Australian economy and society
- Cooperating with neighbours to better respond to cyber incidents
- Improving public-private mechanisms for cyber threat sharing and blocking
- Supporting Australia's cyber security workforce and skills pipeline
- Harmonising regulatory frameworks and reporting obligations
- Introducing a new Cyber Security Act
- Amending the *Security of Critical Infrastructure Act 2018 (Cth)* (SOCI Act).



auDA's contribution:

In our submission on the Cyber Security Strategy (read our [submission highlights](#)), we address some of those key issues by emphasising the importance of:

- Considering cyber security policy and strategy in the context of the digital economy and society, not solely from a national security perspective
- Adopting a human-centric approach to cyber security policy and strategy by striving to make Australians' digital lives more secure
- Supporting the security of the internet including the Domain Name System (DNS) as infrastructure that underpins the digital economy
- Adopting a whole-of-nation approach towards cyber security through multi-stakeholder engagement and discussions
- Streamlining cyber security obligations and laws nationally
- Building regional cyber resilience through bi- and multilateral arrangements in the Asia-Pacific
- Harmonising rules and obligations with relevant laws and frameworks adopted by likeminded jurisdictions.

The [next phase](#) of the Cyber Security Strategy is in motion and stakeholders are awaiting the release of the final version in 2023. In the meantime, the [cyber security coordinator appointment](#) was announced by the Department on 23 June 2023.

Digital identity

In February 2023, at the [Data and Digital Ministers](#) meeting, policymakers and regulators agreed to modernise [Australia's Digital Identity scheme](#) ('scheme'). In May 2023, [AU\\$26.9 million](#) was allocated to expand and update the scheme from the 2023-24 federal budget.

On 23 June 2023, the [National Strategy for Identity Resilience](#) was released by the Department of Home Affairs. It consists of ten principles to guide identity resilience and strengthen identity security arrangements. In other words, it sets out principles and initiatives to make Australians' identities hard to steal and, if compromised, easy to restore.

The Digital Transformation Agency (DTA) continues to lead the development of the scheme and draft legislation is expected to be released later this year. The DTA is also responsible for the [Trusted Digital Identity Framework](#), an accreditation framework ensuring all identity providers meet rules and standards for accessibility, privacy protection, security, risk management and fraud control.



The [Department of Home Affairs says](#) it continues collaborating with the DTA and relevant Commonwealth, state and territory agencies in developing the scheme to ensure it takes a security-by-design approach.

auDA's contribution:

In our [submission on the DTA's Position Paper on Proposed Digital Identity Legislation](#), we expressed our support of a Digital Identity scheme that takes a human-first approach. Australians require accessible and verifiable digital identities that increase security and privacy, tailor the amount of information needed to consume services, and limit the amount of personal information collected and retained by governments and businesses.

We continue to closely monitor this policy area. We will share more detailed views in response to further consultations.

Digital technologies

Key areas of concern to policymakers are digital platforms and artificial intelligence (AI) – two issues that are closely intertwined.

Due to the current and future implications of AI and digital platforms on the wider internet ecosystem and its governance, we take an interest in and monitor such policy matters.

Digital platforms

The Australian Consumer and Competition Commission (ACCC) continues its [Digital platform services inquiry 2020–25](#) ('inquiry'), looking into policy areas including market competition, consumer harm, market trends and innovation as they relate to digital services and platforms. The final report is expected to be provided to the Treasurer by 31 March 2025.

In the context of the ACCC's inquiry, earlier this year, [Treasury requested feedback on the ACCC's regulatory reform recommendations](#). The Treasury was particularly interested in coordination with other government policies and processes, consumer harms and mitigation measures, and other jurisdictions' frameworks.

In June 2023, the Department of Infrastructure, Transport, Regional Development, Communications and the Arts released a [Draft Bill on misinformation and disinformation](#) suggesting that digital platforms' voluntary misinformation and disinformation codes should remain, but also that the Australian Media Communications Authority (ACMA) should be able to deem them ineffective, obtains the power to make an enforceable standards and fine digital platforms for breaches.



The draft bill also proposes providing ACMA with powers to compel platform providers to provide information about their management of misinformation and disinformation.

Artificial intelligence

In May 2023, the House Standing Committee on Employment, Education and Training commenced an [inquiry into the use of generative artificial intelligence in the Australian education system](#). The sector-specific inquiry explores issues and opportunities of generative AI for Australia's education system.

Shortly after, on 1 June 2023, the Department of Industry, Science and Resources (DISR) released its consultation paper seeking views on [Safe and responsible AI in Australia](#) to inform the Government's approach to AI regulation (whether through mandatory or voluntary mechanisms) and risk mitigation.

auDA's contribution:

We responded to Treasury's consultation on ACCC's regulatory reform recommendations, DISR's consultation on safe and responsible AI (read our [submission highlights](#)), and the House Standing Committee's inquiry into generative AI. In our submissions, we emphasise the need for:

- Regulatory coherence and coordination among domestic policymakers
- Regulatory alignment with international frameworks where suitable
- Adoption of a multi-stakeholder approach to capture all stakeholders' needs
- Assessing security-by-design and privacy-by-design principles for digital technologies such as AI
- Adopting a non-regulatory proportionate risk-based approach towards AI governance that maximises economic and social benefits, and minimises harms.

auDA's tech policy radar

Some of the other public policy matters on our radar are:

Electronic Surveillance Reform: The electronic surveillance powers of government agencies are spread across a range of federal and state legislation,² which are subject to varying and inconsistent thresholds and requirements. Some of those laws were

² The *Telecommunications (Interception and Access) Act 1979* (Cth); *Surveillance Devices Act 2004* (Cth); *Australian Security Intelligence Organisation Act 1979* (Cth); and *Telecommunications Act 1997* (Cth); other Commonwealth and state and territory laws.



drafted based on technological assumptions dating back to the 1970s and therefore struggle to keep up with the current pace of technology development. The AGD is leading this reform work, with further proposals expected later this year.

Copyright enforcement review 2022–23: [Public responses to the latest review](#) of Australia's copyright enforcement regime indicate that there is widespread support for improvements to Australia's copyright laws. Based on feedback received, the AGD is developing reform options for:

- Reducing barriers for Australians to use of the legal system to enforce copyright, including examining simple options to resolve 'small value' copyright infringements
- Improving understanding and awareness about copyright.

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

auDA is closely monitoring the multiple trajectories leading up to the development of the [Global Digital Compact](#) (GDC) to be decided at the [Summit of the Future](#) in 2024.

To inform the GDC's design, several consultation streams are underway, including a consultation led by the [UN Tech Envoy's office](#) and an [intergovernmental process](#) led by Rwanda and Sweden.

In May 2023, the UN Secretary-General António Guterres released a [Policy Brief](#) which outlined his vision for digital cooperation and for the GDC. It makes frequent references to another document, prepared by the [High Level Advisory Board on Effective Multilateralism](#) (HLAB Report) which takes a broader look at what a renewed multilateral system for the world would look like.

auDA's contribution:

auDA together with several stakeholders of the Australian Internet Governance community [submitted a contribution to the GDC](#) supporting the multi-stakeholder model for internet governance and the Internet Governance Forum (IGF) as a valued platform for internet governance discussions. We are developing our analysis of the



Secretary-General's Policy Brief and expect to offer public comments on it in August 2023.

ICANN 77

In June 2023, we participated in the 77th ICANN forum (ICANN77) in Washington, DC, and joined global multi-stakeholder discussion and collaboration on the latest developments in the internet ecosystem.

Following the event, [auDA hosted a debrief webinar](#) with forum participants from ICANN's various Supporting Organisations and Advisory Committees to hear their perspectives on ICANN77. Topics addressed include:

- Combatting DNS abuse
- The next round of new generic top-level domains
- The progression of internationalized domain name policy (or domain names in local language scripts such as .クラウド which stands for .cloud in Japanese)
- A new appeals process relating to ICANN decisions on country code top-level domains.

The next ICANN meeting will be held on 21-26 October 2023 in Hamburg, Germany. In the meantime, you can read our [ICANN77 meeting report blog](#).

EuroDIG

We attended the [European Dialogue on Internet Governance \(EuroDIG\) 2023](#) in Tampere, Finland, from 19-21 June.

EuroDIG is an annual multi-stakeholder conference in Europe that closely follows the United Nations' IGF. The events highlighted the importance of collaboration, education, inclusivity, and a multi-stakeholder approach to address digital challenges and promote a secure and open digital future for everyone.

The 2023 EuroDIG program reflected the theme "Internet in troubled times: risks, resilience, hope". Internet fragmentation was a dominant subject. The agenda also included topics not traditionally associated with internet governance, though currently salient, such as AI and platform regulation, and digital literacy to counter misleading information.

Internet & Jurisdiction

On 11-12 May, auDA participated in work by the Internet & Jurisdiction Policy Network to develop shared approaches to how domain name registries could deal with emergency content problems - including when such action might be appropriate.



Global Policy: what's happening overseas?

The European Union's AI Act

The European Parliament's vote to approve its draft rules for the AI Act passed with an overwhelming majority in June 2023. The AI Act has been welcomed as one of the world's most important developments in AI regulation, that may possibly set the global standard for years to come. The AI Act will likely take around two years for the laws to be implemented.

The AI Act takes a risk-based approach by introducing restrictions based on how dangerous lawmakers predict AI applications to be. Those AI applications posing "unacceptable" risk will be banned entirely, while those deemed "high risk" will have new limitations on their use and requirements around transparency.

Find out more: [Artificial Intelligence Act](#)

The European Union's Cyber Resilience Act

The Cyber Resilience Act (CRA) is intended to strengthen cyber security for all Europeans. It is set out to establish minimum cybersecurity requirements for the vast majority of products and services connected to the internet. From this perspective, it will be the first 'Internet of Things' (IoT) legislation in the world.

The CRA divides digital products into two main categories, based on their risk level. The first is 'default non-critical products', i.e. hardware and software with a low level of criticality (e.g. smart home assistants, connected toys). The second is 'critical products', which are further divided into [two sub-categories](#), *class I lower risk* (e.g. virtual private networks and routers) and *class II higher risk* (e.g. operating systems for desktops and mobile phones or smart meters) reflecting criticality and intended use.

Critical products have to comply with stricter obligations than other products. The CRA requires software providers to adhere to new cyber security requirements. It also places requirements on device manufacturers and distributors with regards to vulnerability disclosure and introduces new liability regulations for cyber security incidents.

Find out more: [Cyber Resilience Act](#)

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: [Fragment or Not Fragment – Is This the Question? Will the “One World–One Internet” Survive Today’s Geopolitical Stress Tests?](#)

- **What’s it about:** The need to reinforce the multi-stakeholder approach and uphold ICANN and the IGF to sustain the concept of “One World – One Internet” as we know it. In other words, the article highlights the importance of avoiding internet fragmentation and splintering the global internet at all costs – for everyone’s benefit.
- **Why we are interested:** A split internet, divided along ideological lines, is a bad thing, but not an unrealistic option. As advocates for an open, free, secure and global internet, we strongly support the multi-stakeholder approach. As noted in our GDC submission, the GDC is a great opportunity to reach a new quality in multi-stakeholder cooperation.

Title: [Déjà Vu: Is the UN Attempting to Take Over the Internet \(Again\)?](#)

- **What’s it about:** Countries including Russia and China imposing their version of a censored internet by pushing for “top-down” internet controlled by the UN.
- **Why we are interested:** UN Secretary-General Guterres seems open to such proposals. The GDC includes a call to establish a new UN-run Digital Cooperation Forum. We believe that such an approach would pose significant risks to an open, free, secure and global internet.

Title: [The EU AI Act: A Critical Assessment](#)

- **What’s it about:** The article explores what it considers the flawed regulatory approach towards AI taken by the EU in contrast with other (non-)regulatory proposals by other jurisdictions including Australia, China and the United States.
- **Why we are interested:** We closely monitor the development of AI regulations and laws across the world. Although the EU AI Act is said to set ‘global standard’ for AI regulation, we believe that a proportionate risk-based approach that is innovation-friendly should be the preferred approach.



What's coming up in Q3 2023?

Events

15-16 August 2023

International Institute of Communications (IIC) Telecommunications and Media Forum

At this in-person event in Sydney, [IIC](#) members, regulators, policymakers and industry participants come together to discuss policy matters including AI governance, digital platforms, online safety, cyber security, consumer data protection, scams and fraud (see [agenda](#) for more information).

28-31 August 2023

Asia Pacific Regional Internet Governance Forum (APrIGF) and NetThing

auDA is excited to bring the 2023 APrIGF to Australia (Brisbane) for the first time. The APrIGF is a regional level internet governance and policy forum for the Asia Pacific. Emerging technologies is the key theme. The 5th Annual [NetThing Forum on Internet Governance and Technology](#) will be held in conjunction with the APrIGF. [Browse the program](#) and [register](#) for NetThing (28 August) and the APrIGF (29-31 August).

18-20 September 2023

Asia Pacific Top Level Domain Association (APTLD)

[APTLD](#) is an organisation for ccTLD (country-code Top Level Domain) registries in the Asia Pacific region. Topics including automation of ccTLD processes, GDPR for ccTLDs, innovation and digitalisation, splinternet and ESG, are on the [agenda](#). The event takes place in Seoul, Korea.

Webinars

16 August 2023

Launch of auDA's Internet Governance Roadmap

The rapid growth of the internet has led to new challenges and opportunities. Join our webinar where we will discuss these issues and launch auDA's Internet Governance Roadmap, part of our contribution to the dialogue (register [here](#)).

11:00am - 12:00noon AEST (Melbourne, UTC+10)

Policy

auDA's first Internet Governance Roadmap

Shortly, auDA will release its Internet Governance Roadmap 2023-2025. Our Internet



Governance Roadmap shares auDA's analysis of the current state of multi-stakeholder internet governance and proposes action to improve it.

Open consultations – have your say

Agency	Consultation	Submission due date
Department of Infrastructure, Transport, Regional Development, Communications and the Arts	Exposure Draft of the Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2023	20 August 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.