What's Ahead: 2025 Digital Economy in Australia

Digital platforms, online content providers and other businesses active in the digital economy continue to face an increasingly complex and evolving regulatory and legal landscape in Australia. 2025 will see the AI hype continue, as businesses vie to unlock the full potential of AI, innovation continues at pace, and governments strive to strike the right balance between fostering AI investment and addressing potential harms. Here is our take on key themes this year:

1. **A regulation reset**: The tech regulatory landscape in the US – and potentially globally – faces a significant shift under the Trump administration. The administration's deregulatory stance is likely to see AI regulation and data privacy laws slow down in the US, while content moderation / censorship will be a hot topic. But its impact is likely to also be felt outside the US: the administration has raised concerns about foreign laws that "discriminate against innovative American companies", including the EU's DMA and DSA. It has indicated that the US will "impose tariffs" and take other "actions necessary" in response to foreign governments that impose burdens on US companies through their taxes or regulatory structures.

   Against a backdrop of slowing growth in Europe and the UK, a renewed focus on enabling investment and innovation is emerging. Mario Draghi's report on the future of European competitiveness and the UK Government's recent directive to regulators suggest we will see greater scrutiny of recently introduced tech regulation, and a more light touch approach going forward (for example, in respect of AI). Just how this sentiment (and the Trump effect) will impact the Government's reform agenda in Australia remains to be seen. With a Federal election taking place by May, the outcome of proposals currently before the Government (such as the proposed "Digital Duty of Care") are even harder to predict and prepare for.

2. **Uptick in M&A activity**: All signs point to a continued uptick in tech M&A, driven by private equity, maturing of venture backed technology companies, lower interest rates, corporates with a continued focus on harnessing the benefits of innovation, digital innovation and automation, and investment in digital infrastructure, including data centres. A more 'business friendly' approach in the US, and a moderating regulatory environment in the UK, will encourage global dealmakers. We may see a rush of local deals ahead of the commencement of Australia's new merger control regime in 2026.

3. **Continued scrutiny and harms-based action by regulators**: Australia's Digital Platforms Regulators Forum (DP-REG), and its constituents, will continue their focus on digital platforms and emerging risks. The Australian Competition and Consumer Commission's (ACCC) enforcement priorities for 2025 include competition, product safety, consumer and fair-trading issues in the digital economy, with a focus on misleading advertising within influencer marketing, online reviews, in-app purchases and unsafe consumer products. Similarly, Australia's privacy regulator has a focus on online platforms, social media and high privacy impact technologies. Across the board, regulatory action will be focussed on high-risk matters with the greatest potential for harm.

4. **More private actions**: Recent years have seen an uptick in private proceedings, including class actions, alleging breaches of competition and consumer laws, data breaches and privacy claims. The Federal Court's decision on Epic's proceedings against Apple and Google (and related class actions) regarding mobile app distribution is expected in H1, and data breach class actions against Optus and Medibank continue to progress through the Federal Court. There is an increase in litigation worldwide in relation to infringement of copyright in the training of AI models. A statutory tort for serious invasions of privacy will be available by June 2025, providing a new avenue for private actions for damages.

What's Ahead: 2025 Digital Economy in Australia

AI

1. **Mandatory guardrails for AI in high-risk settings**: The Australian Government is expected to finalise its regulatory framework for mandatory guardrails for AI in high-risk settings, following the September 2024 release of a Voluntary AI Safety Standard outlining 10 voluntary guardrails, and a proposal paper detailing 10 closely aligned mandatory guardrails for high-risk settings.
2. **National AI Capability Plan**: Due to be delivered at the end of 2025 following consultation, the plan will detail how Australia will grow investment, strengthen AI capabilities and boost AI skills, and secure economic resilience.
3. **AI ACL Review**: In November 2024, Treasury completed a consultation on whether the Australian Consumer Law (ACL) remains suitable to protect consumers who use AI-enabled goods and services, and to support the safe and responsible use of AI by business. We expect Treasury to publish the outcome of its review this year.
4. **EU AI Act gradually implemented**: From 2 February 2025, key provisions of the EU AI Act (which has extraterritorial impact) became applicable to companies that offer or use AI systems in Europe. From 2 August, the imposition of fines will be possible. Signalling a shift in Europe's tech regulation policy, the proposed AI Liability Directive was withdrawn in February 2025.
5. **Tensions between AI developers and content creators**: 2024 saw the announcement of several licensing partnerships between AI models and news outlets, but copyright issues around content used for training AI models remain contentious, with high profile cases underway in the US, UK and Canada. In the UK, a voluntary AI Code of Practice was abandoned, and the UK Government recently concluded consultation on a new copyright and AI framework.
6. **Space for innovation?** In a joint statement with Korea, Japan, France, Ireland and the UK, Australia's Privacy Commissioner has committed to reducing legal uncertainties and securing space for innovation (which might include things like regulatory sandboxes), to fostering a clear international understanding of lawful grounds for processing data to train AI, and to continued information sharing and collaboration between regulators.
7. **AI hype and dynamism continue, but security and privacy concerns loom large**: Advancements in LLMs and generative AI continue at pace, with the emergence of smaller, more efficient models, enhanced multimodal capabilities and specialised models. DeepSeek made waves in the industry earlier this year, and was soon banned from all government systems and devices in Australia, following security and privacy concerns. Regulators in South Korea, Ireland and France have all begun investigations into how DeepSeek handles user data, stored on servers in China.

Privacy and Data

1. **Ongoing privacy reforms**: Tranche 1 of reforms to Australia's Privacy Act passed in November 2024 and will progressively take effect, but wider-reaching tranche 2 reforms won't progress until after the Federal election.
2. **A new-look privacy regulator**: The Australia's privacy regulator intends to complete its transition to a smaller and more focussed structure, targeting high-risk activities with a greater potential for harm, and exercising new enforcement and investigation powers. Expect a more proactive approach, as well as a focus on closing out long-running matters, such the settlement of proceedings against Meta for a record $50 million package (in December 2024).
3. **Children's Online Privacy Code**: A new Children's Online Privacy Code is being prepared by the privacy regulator, to be released for at least 60 days of consultation, and finally registered by 10 December 2026. Where possible, the code is expected to align with the UK's Age Appropriate Design Code.
4. **New action for invasion of privacy**: A new statutory tort allowing individuals for the first time to take direct legal action for a serious invasion of privacy (not limited to a breach of Australia's Privacy Act) will come into force no later than June 2025. We expect to see claims for damages in a variety of situations including claims arising out of data breaches and social media.
5. **Digital ID**: Laws for Australia's Digital ID accreditation and the government myID system commenced 1 December 2024. Expect increasing use of Digital ID in the private sector, with participation in the Government system within 2 years, a consultation on expanded use of Digital ID in telecommunications, and Australian banks trialling identity verification using a digital Medicare card.
6. **Consumer data right (open data)**: After a pause and reset of the regime in late 2024, we'll see a focus on high impact banking and energy use cases, a narrowing of banking data scope, and expansion to non-bank lenders in the second half of 2026. The CDR is still looking for its "killer app".

Key cases to watch

- **New York Times v OpenAI and Microsoft**: filed in the US in December 2023, alleging that the training of Open AI infringed New York Times copyright. Similar proceedings were brought by five major news organisations in Canada, in 2024.
- **Getty Images v Stability AI**: filed in the US and UK alleging that Stability AI's Stable Diffusion system that generates images infringed copyright by using Getty images as data inputs for training purposes.
- **OAIC v Australian Clinical Labs**: alleging failure to ensure the security of personal information and to satisfy data breach notification obligations. This is the first data breach matter for the OAIC to seek civil penalties. Hearing expected in October 2025.
- **Optus, Medibank and Latitude**: each facing regulatory action, class action, and/or representative complaints following major cyber incidents.
- **Bunnings v OAIC**: the OAIC determined Bunnings' use of facial recognition breached privacy obligations. Bunnings has sought review, with a hearing in October 2025.

What's Ahead: 2025 Digital Economy in Australia

Competition and Consumer Protection

1. **New Merger Control Regime**: The *Treasury Laws Amendment (Mergers and Acquisitions Reform) Bill 2024* passed, transforming Australia's current, voluntary, merger system. The new regime will commence on 1 January 2026, but will become available on a voluntary basis from 1 July 2025. Merger clearance will become mandatory and suspensory for transactions that exceed specified monetary thresholds. Treasury has announced its intended financial thresholds, but further consultation is expected as the subordinate legislation is developed this year. The Minister will have the power to require certain high-risk acquisitions (in certain sectors, or by certain entities) to be notified according to lower thresholds. The ACCC will release draft process and analytical guidelines, and Treasury is expected to consult on notification forms, by the end of Q1 2025.
2. **Ex Ante Digital Platform Regulation**: Treasury is consulting on a proposed new digital competition regime. The proposal is a hybrid of the EU's DMA and the UK's DMCC Act, with broad obligations to be embedded in the *Competition and Consumer Act 2010* (CCA) and service-specific obligations in subordinate legislation. It would apply to digital services designated by the Treasurer, and be enforced by the ACCC, with Court oversight. Services potentially in scope include app stores, online advertising services (including ad tech), social media, operating systems, search engine services, and cloud services, among others. Maximum penalties are proposed to match those under the CCA: $50 million, 3x the value of the benefit obtained, or 30% of adjusted turnover during the breach period. We expect Treasury to publish the outcome of its consultation and exposure draft legislation this year.
3. **Scams Prevention Framework (SPF)**: The *Scams Prevention Framework Bill 2025* passed, and the SPF came into effect on 20 February 2025, as new Part IVF of the CCA. The SPF establishes six scam prevention principles (governance, prevent, detect, report, disrupt and respond) which designated sectors must adopt. Industry codes will follow with industry-specific obligations. Social media, paid search engine advertising and direct messaging (along with telecommunications and banking) will be initially designated. Maximum penalties for "Tier 1". breaches will match those under the CCA (see above). The ACCC will enforce the framework and the digital platforms sector scams code.
4. **Unfair Trading Practices**: In December 2024, Treasury completed its supplementary consultation on amending the ACL to add a general, principles-based prohibition on unfair trading practices (which could capture 'unreasonable use' of dark patterns that are likely to cause 'material consumer detriment'), and specific prohibitions targeting certain unfair practices (subscription-related practices, drip pricing, dynamic pricing, online account requirements and barriers to accessing customer support). While the prohibitions would apply economy-wide, they are of particular relevance to many online practices. We expect Treasury to publish the outcome of its consultation, and potentially exposure draft legislation, later this year.
5. **News Bargaining Incentive**: In December 2024, the Albanese Government announced its intention to establish a "News Bargaining Incentive" (or levy), acknowledging the limitations of the News Media Bargaining Code introduced in 2021. The incentive is intended to apply to large digital platforms operating significant social media or search services, to encourage entry into commercial deals with news publishers. A public consultation paper will be released early this year.
6. **ACCC Digital Platform Services Inquiry (DPSI)**: The 5-year inquiry is coming to an end, with the ACCC's 10th report due on 31 March 2025. The report will cover recent international legislative and regulatory developments in markets for digital platform services and their impact on competition and consumers, major developments in online private messaging and app stores, and emerging issues (including in online gaming, cloud computing and generative AI).
7. **Continued scrutiny by the ACCC's Digital Platforms Branch**: In 2024, the ACCC accepted court-enforceable undertakings from Telstra, Optus and TPG as part of an ongoing competition investigation into Google's search services in Australia. The branch is also reportedly investigating Apple's restriction of third-party access to NFC technology and Apple Pay terms, and Google's ad tech business. Competition, product safety, consumer and fair trading issues in the digital economy are an enforcement priority for the ACCC in 2025.

Key cases to watch

- **ACCC v Meta**: alleging misleading or deceptive conduct by publishing scam advertisements promoting cryptocurrency investment schemes featuring prominent Australian public figures.
- **ACCC v eHarmony**: alleging misleading or deceptive conduct in relation to membership services, including autorenewal and early cancellation.
- **ACCC v Webjet**: alleging misleading representations about minimum flight prices, which omitted compulsory fees, and booking confirmations.
- **Epic / Google / Apple litigation and class actions**: alleging app stores have misused their market power and engaged in unconscionable conduct by restricting distribution and imposing a 30% commission. Judgment expected in H1.
- **Sony Interactive class action**: alleging Sony abused its market power by overcharging for the creation and purchase of digital content through the PlayStation Store, and imposed restrictive T&Cs to eliminate competition.
- **Ad Tech class actions**: two class actions have been filed against Google alleging abuse of dominance in digital advertising.
- **Dialogue Consulting v Instagram**: alleging withdrawal of access to products constituted misuse of market power, misleading conduct and unconscionable conduct.

What's Ahead: 2025 Digital Economy in Australia

Online Safety

1. **Online Safety Review Report**: Released February 2025, containing 67 wide-ranging recommendations. The Government has acted on some (eg increased penalties, social media minimum age) and committed to others (eg Digital Duty of Care).
2. **Increased penalties change the risk profile**: Maximum online safety penalties (eg for industry codes or standards) were increased from AUD$825,000 to AUD$49.5m in December 2024.
3. **Age assurance in the spotlight**: Identifying children underpins incoming social media minimum age laws and eSafety and Children's Online Privacy Codes. Australia's age assurance technology trial will report mid-2025. eSafety's transparency report summarised findings of information requests to social media platforms issued in September 2024. Several US states have proposed age assurance at the device or app store level, Google will test age estimation by machine learning, and Apple will introduce tools to allow parents to share their child's age range and limit app use by age range.
4. **Social Media Minimum Age**: New laws will require impacted social media platforms to take reasonable steps to prevent persons under 16 years of age from having an account – new laws are expected to take effect before 11 December 2025, and will be supported by eSafety guidance.
5. **New eSafety codes**: New standards for seriously harmful content such as child exploitation and pro-terror materials came into effect 21 December 2024, completing the first tranche of codes and standards. A second tranche aimed **at** age-restricted content is in developments – 7 draft codes have been submitted to the Commissioner, with a further code due by 28 March 2025.
6. **Digital Duty of Care**: The Government has floated a Digital Duty of Care requiring digital platforms to take reasonable steps to prevent foreseeable harms, underpinned by risk assessment and risk mitigation, and informed by safety-by-design principles.
7. **Extremist content**: A Senate report recommended best practice guidelines for assuring that social media platforms enforce terms of service to exclude harmful extremist content.
8. **Misinformation and disinformation bill abandoned**, leaving in place the voluntary industry code.

Cyber security

1. **Australia's world-first ransom reporting regime**: New laws include a new Cyber Security Act 2024 with mandatory ransom payment reporting, new security standards for smart (IoT) devices, limits on how cyber agencies use cyber incident information, and the creation of a Cyber Incident Review Board. Underlying regulations are expected to be made soon.
2. **Critical infrastructure reform**: New security of critical infrastructure laws passed in late 2024 will expand the Security of Critical Infrastructure Act 2018 to the telecommunications sector, give greater powers to the Department of Home Affairs in relation to critical infrastructure risk management programs, adjust the rules for assets storing critical data, and streamline the sharing of protected information.
3. **ASIC targeting directors**: Australia's corporations regulator expects effective cyber security risk management and resilience. With active investigations already underway, expect more enforcement action in 2025.

Telco and satellite

1. **Telco law refresh**: In a move that will impact digital economy businesses operating subsea cables and satellite services as well as traditional consumer telco businesses, a Government bill proposes broad changes including registration scheme for carriage service providers, a shift towards mandatory and directly enforceable industry codes and standards, and an increase to maximum penalties to the greater of $10m, three times the benefit of a breach, or 30% of turnover for the period.
2. **Telco in the spotlight**: The ACCC's enforcement priorities include promoting competition and combatting misleading pricing and claims in essential services (including telecommunications). The Australian Communications and Media Authority continues to focus on protecting customers. Network security and resilience will move from industry specific legislation into the Security of Critical Infrastructure regime, bringing updated obligations, new regulatory expectations, and regulatory oversight – coming into effect before November 2025.
3. **Low Earth Orbit satellite**: Reviews over the past year have focussed on how Australia delivers and funds essential connectivity, and emphasised the need to explore technology options including LEO. The Government has announced a Universal Outdoor Mobile Obligation plan to deliver ubiquitous mobile voice and sms coverage using LEO satellite direct-to-device technology.

Key cases to watch

- **eSafety v X Corp:** alleging failure to comply with a transparency notice under the Online Safety Act.
- **eSafety v Telegram:** eSafety issued an infringement notice for almost $1 million to Telegram, for failing to respond to a transparency notice, and delaying the publication of critical information about steps taken to address any terrorist and violent extremist, and child sexual exploitation, material on the platform.

Thought leadership

Ashurst is committed to keeping clients informed on key regulatory and policy developments in the evolving digital landscape. Our thought leadership provides clients with insights into these changes through exclusive roundtable discussions and in-depth articles. From regulatory resets and evolving AI policies to M&A trends and increasing regulatory scrutiny, we help businesses stay ahead of the curve and prepare for what's next.

Horizon Scanning

Recent activities have included:

Artificial Intelligence

- EU AI Act: deadline for prohibited AI systems is fast approaching, 31 January 2025
- Board Priorities in 2025: Artificial intelligence, 16 January 2025
- Australia: New AI safety "guardrails" and a targeted approach to high-risk settings, 28 November 2024
- Global AI Regulation Guide, 28 November 2024

Privacy and Data

- Australian Privacy Reforms: A generational change inches closer, 17 December 2024
- Navigating Data Protection Reforms: A Comparative Analysis of UK and Australia, 12 December 2024
- Outpacing cyber laws – Redefining cyber readiness, 17 October 2024
- Australia's first tranche of privacy reforms – a deep dive and why they matter, 15 October 2024

Competition and Consumer Protection

- More with more: ACCC announces bumper compliance and enforcement priorities for 2025-26, 21 February 2025
- Merger reforms passed by Australian Parliament, 29 November 2024
- Australian government moves to ban unfair trading practices, 18 November 2024
- Australia's bold Scam Prevention Framework Bill has been introduced into Parliament, 15 November 2024
- The long awaited Scam Prevention Framework is here!, 2 October 2024

Tech M&A

- What to Expect for Tech M&A in 2025, 23 December 2024
- Tech M&A: Recent "Acquihires" in the Tech Sector, 13 August 2024
- Tech M&A: Key Pitfalls to Anticipate and Avoid With Deferred Consideration, 3 June 2024

Disputes

- Current trends in Australian disputes 2024-25, 31 January 2025
- Declassing class actions: Reflections following the Waller Legal class action, 5 March 2025

Cyber Security

- Redefining cyber readiness – Australia passes its first Cyber Security Act, 28 November 2024
- Changes to the SOCI Act are on the horizon, 22 October 2024
- Redefining cyber readiness – Three ways to outpace Australia's new cyber laws, 10 October 2024
- Governing Through a Cyber Crisis - Cyber Incident Response and Recovery for Australian Directors (aicd.com.au), February 2024

Key contacts

Competition

Tihana Zuk
Partner
T +61 2 9258 6343
tihana.zuk@ashurst.com

Peter Armitage
Partner
T +61 2 9258 6119
peter.armitage@ashurst.com

Digital Economy Transactions

Rebecca Cope
Partner
T +61 2 9258 6085
rebecca.cope@ashurst.com

Geoff McGrath
Partner
T +61 2 9258 6816
geoff.mcgrath@ashurst.com

Dispute Resolution

Nicholas Mavrakis
Partner
T +61 2 9258 6501
nicholas.mavrakis@ashurst.com

Ian Bolster
Practice Head,
Dispute Resolution,
Australia
T +61 2 9258 6697
ian.bolster@ashurst.com

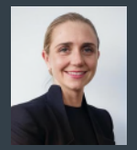
IP / Media

Nina Fitzgerald
Partner
T +61 2 9258 6778
nina.fitzgerald@ashurst.com

Robert Todd
Partner
T +61 2 9258 6082
robert.todd@ashurst.com

Corporate Transactions

Stuart Dullard
Partner
T +61 2 9258 6536
stuart.dullard@ashurst.com



Brooke Coghlan
Partner
T +61 3 9679 3626
brooke.coghlan@ashurst.com

Risk Advisory

John Macpherson
Partner, Cyber,
Risk Advisory
T +61 2 9258 6479
john.macpherson@ashurst.com

Sonia Haque-Vatcher
Partner, Data & Analytics
Risk Advisory
T +61 2 9258 5948
sonia.haque-vatcher@ashurst.com

Expertise

Andrew Hilton
Expertise Counsel
T +61 2 9258 6338
andrew.hilton@ashurst.com

Amanda Tesvic
Expertise Counsel
T +61 2 9258 5696
amanda.tesvic@ashurst.com

This publication is a joint publication from Ashurst Australia and Ashurst Risk Advisory Pty Ltd, which are part of the Ashurst Group.

The Ashurst Group comprises Ashurst LLP, Ashurst Australia and their respective affiliates (including independent local partnerships, companies or other entities) which are authorised to use the name "Ashurst" or describe themselves as being affiliated with Ashurst. Some members of the Ashurst Group are limited liability entities.

The services provided by Ashurst Risk Advisory Pty Ltd do not constitute legal services or legal advice, and are not provided by Australian legal practitioners in that capacity. The laws and regulations which govern the provision of legal services in the relevant jurisdiction do not apply to the provision of non-legal services.

For more information about the Ashurst Group, which Ashurst Group entity operates in a particular country and the services offered, please visit www.ashurst.com

This material is current as at 4 March 2025 but does not take into account any developments to the law after that date. It is not intended to be a comprehensive review of all developments in the law and in practice, or to cover all aspects of those referred to, and does not constitute legal advice. The information provided is general in nature, and does not take into account and is not intended to apply to any specific issues or circumstances. Readers should take independent legal advice. No part of this publication may be reproduced by any process without prior written permission from Ashurst. While we use reasonable skill and care in the preparation of this material, we accept no liability for use of and reliance upon it by any person.

The information provided is not intended to be a comprehensive review of all developments in the law and practice, or to cover all aspects of those referred to.
Readers should take legal advice before applying it to specific issues or transactions.