Ashurst

What's Ahead

2026 Technology industry in Australia

Outpacing change

Introduction

Technology businesses operating in Australia continue to face a rapidly evolving landscape. Global disruption and regulatory divergence, unprecedented investment in infrastructure fuelled by AI, heightened merger scrutiny, and a surge in private legal actions are shaping a complex environment where innovation, compliance, and risk management must be carefully balanced.

1. **Navigating global divergence:** The global tech regulatory landscape is entering a period of heightened divergence, as the US and EU move in opposite directions, leaving middle-ground jurisdictions like Australia to navigate a complex path between innovation-led growth and safety-first oversight.

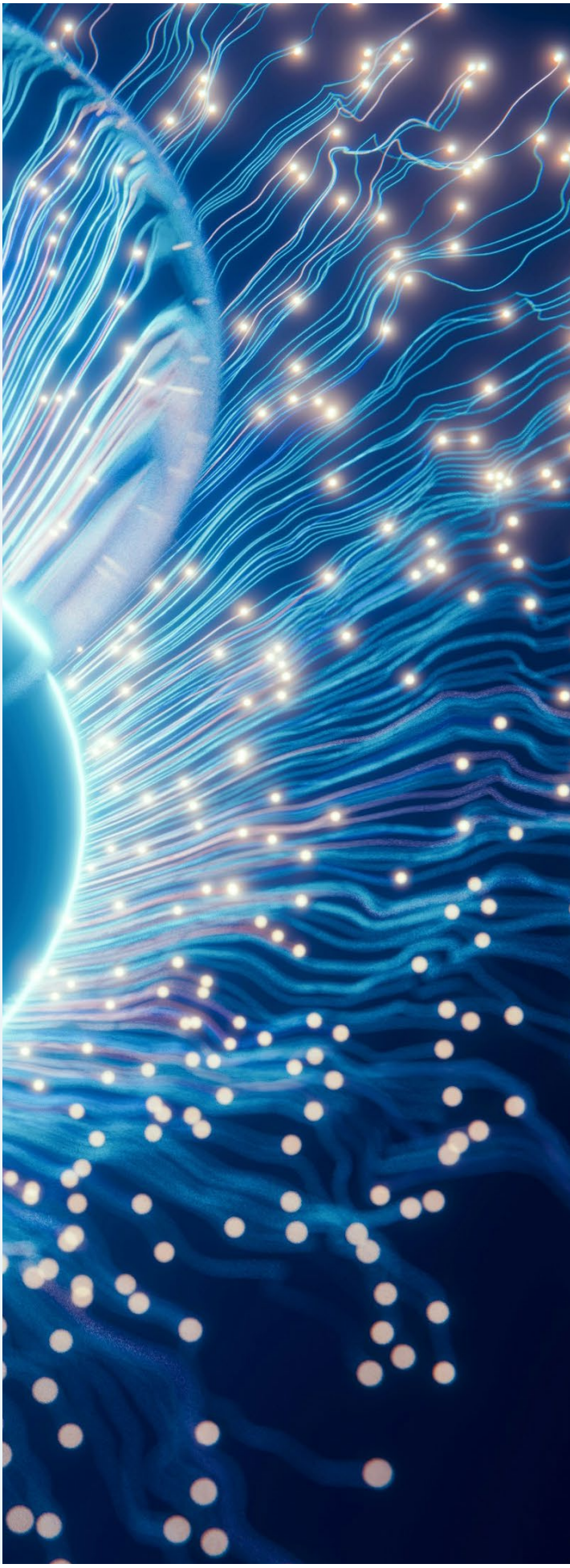
    - In the US, the Trump administration is using executive orders and agency directives to curb the proliferation of "onerous" and "excessive" state-level AI laws in favour of a single, innovation-first national framework. The administration has also sharpened its rhetoric against foreign digital regulation, continuing to single out the European Commission (alongside other foreign governments) and threatening to deploy "every tool at its disposal" (including tariffs) to retaliate against what it describes as "discrimination" against US firms.
    - Despite US pressure, the European Commission refuses to "undo" digital regulation and plans to step up its enforcement of the Digital Markets Act (DMA) and Digital Services Act (DSA). The Commission recently imposed significant fines against Google, TikTok and X (formerly Twitter) and continues to investigate Meta's AI policy on WhatsApp, Google's use of web publishers' content for AI Overviews, and whether the DMA should be expanded to cover cloud services. In parallel, the Commission has acknowledged the need for a more simplified digital regulatory framework to avoid the unintended consequences identified in Draghi's report. It continues to consult on its Digital Omnibus Package unveiled in November last year.

    How this global dynamic will shape Australia's own digital reform agenda in 2026 remains to be seen. Under the National AI Plan, Australia will rely on existing, largely technology-neutral legal frameworks, and regulators will monitor and address AI-related harms within their policy and regulatory domains. The proposed digital platform "ex ante" regime remains on the cards, although it is progressing slowly. In practice, we expect closer, more assertive use of established legal frameworks – competition and consumer law, privacy and data protection, online safety, and sector-specific regimes – to address harms, with ongoing monitoring and possibly future targeted regulation where genuine gaps emerge (as we have seen already with respect to scams and unfair trading practices).

2. **New approach to managing data centre growth:** Australia was the second highest recipient of data centre investment in the world in 2024, and investment continues to grow. In September 2025 alone, Australia's quarterly spend on IT machinery and equipment doubled to $2.8bn. Data centres are critical infrastructure in Australia, underpinning economic activity and public services. The unprecedented level of demand for Australian data centres is being fuelled primarily by AI, geopolitics and the impact on regional security and data sovereignty. Such huge demand is feeding rapid growth, and has prompted concerns as to the impact that data centres are having, or will have, on energy demand, electricity infrastructure, water usage, and the environment and local communities. The NSW Legislative Council is conducting an inquiry into these issues, and the federal Government is due to release national data centre principles "early" this year, flagging that key requirements will include additional investment in renewable energy generation and water sustainability.

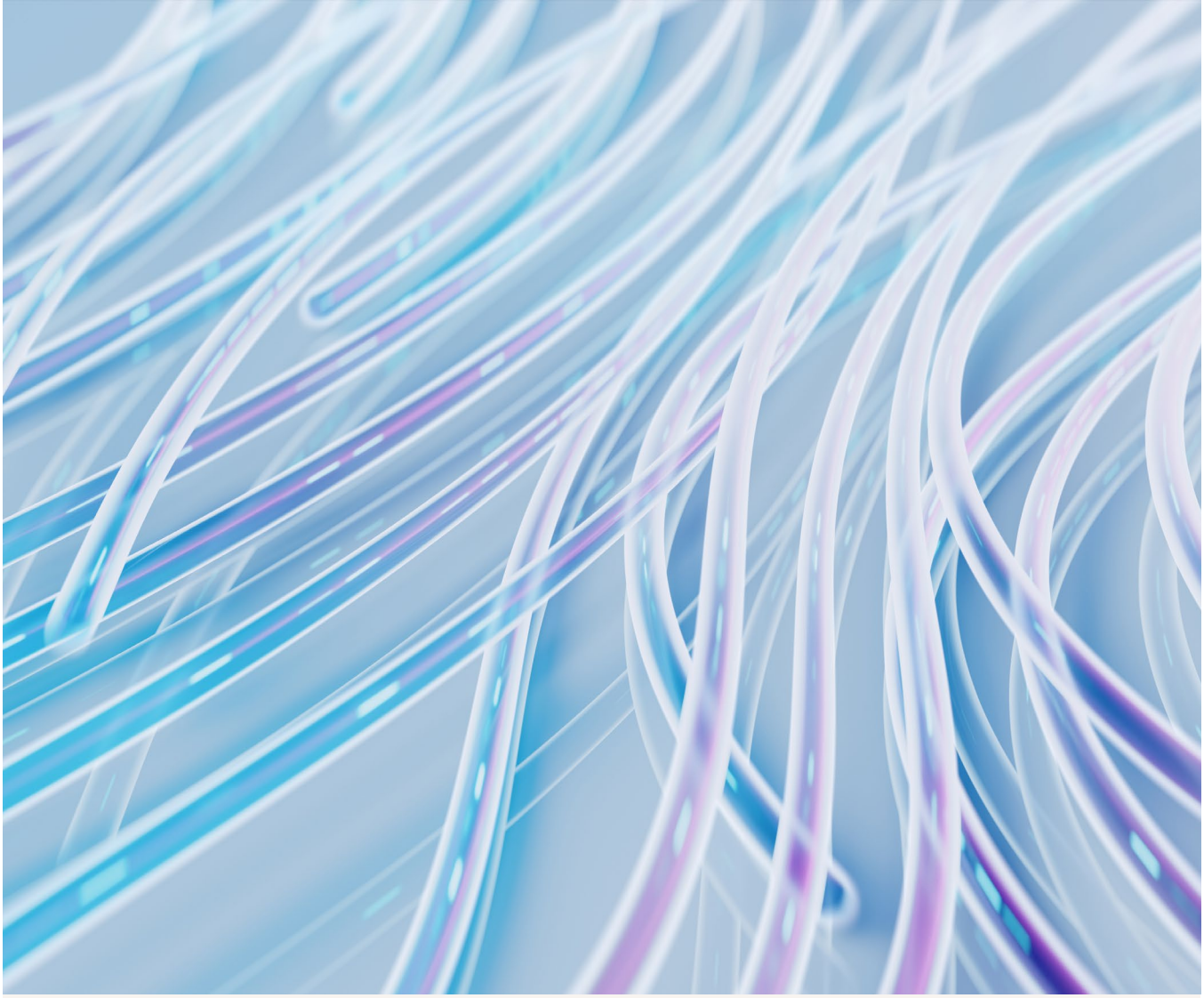
3. **The new mandatory merger reality:** Dealmaking in the tech sector has entered a new era where the Australian Competition and Consumer Commission (ACCC) must be notified of acquisitions meeting specific monetary or "serial acquisition" thresholds, with the transaction legally void and parties facing substantial penalties if closed without clearance. This regime specifically targets the "creep" of market power, meaning that even smaller bolt-on acquisitions by large digital platforms are now under intense scrutiny. The inclusion of intellectual property assets within the regime's scope has also fundamentally changed how technology transfers and licensing deals are structured. Despite this, M&A activity increased throughout 2025 based on available capital and developments in AI investment, and looks set to continue its confident start to 2026.

4. **More private actions:** Private actions in the Australian tech sector are expected to continue to accelerate, fuelled by the Federal Court's August 2025 decision in Epic Games v Apple & Google, the maturation of the new statutory privacy tort, and ongoing scrutiny of AI. The new statutory tort for serious invasions of privacy allows claims outside of Australia's existing privacy framework, and we expect plaintiffs to test boundaries and creatively leverage court processes and remedies (such as interim injunctions and declarations) for tactical advantage. In the realm of intellectual property, Australia's decision not to introduce a text and data mining copyright exemption to enable AI training has created a legal environment distinct to the US or EU, potentially giving Australian creators a stronger hand to bring private actions for copyright infringement.



Competition and Consumer Protection

1	**Merger Control Regime:** A new mandatory and suspensory merger regime commenced on 1 January 2026, requiring clearance for transactions that exceed specified monetary thresholds. Transactions involving targets that supply products to users in Australia, including minority shareholdings or acquisitions of assets such as IP rights may now be notifiable. A 3-year lookback means that even very low value transactions by serial acquirers may be captured (see more detail here).
2	**Ex Ante Digital Platform Regulation:** Consultation on Treasury's proposed new digital competition regime (a hybrid of the EU's DMA and the UK's DMCCA) closed in February 2025, though no draft legislation has been released. The proposed regime would apply to large designated platforms, with app stores and ad tech services prioritised for regulation (with scope for additional services to be added). Under the current proposal, once designated, platforms would be subject to broad obligations under the Competition and Consumer Act 2010 (CCA) and service-specific obligations in subordinate legislation. 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.
3	**Scams Prevention Framework (SPF):** The SPF celebrated its first anniversary on 21 February 2026, though obligations commence only once sectors are formally designated. Treasury proposes designating certain digital platforms (instant messaging, search and social media services), banks and telecommunications providers from 1 July 2026. Regulated entities must then comply with obligations under six principles: governance, prevent, detect, report, disrupt and respond. Further consultation on sector-specific codes is expected in 2026.
4	**Unfair Trading Practices:** The Government has released draft reforms to the Australian Consumer Law (ACL) introducing a general prohibition on practices that unreasonably distort or manipulate consumer decision-making, mandatory disclosure requirements for subscription models, and enhanced transparency for transaction-based charges (targeting "drip pricing"). The reforms are intended to capture "dark patterns" (i.e, interface designs that steer users toward particular choices, like pre-selected checkboxes or unnecessary low stock notifications), complicated cancellation processes, and fees revealed late in the purchasing journey. If passed, the reforms are expected to take effect from 1 July 2027.
5	**News Bargaining Incentive:** In November 2025, almost a year after its announcement, the Government released a consultation paper on its proposed "News Bargaining Incentive" (or levy), designed to address limitations in the News Media Bargaining Code by incentivising large digital platforms to enter commercial deals with news publishers, regardless of whether or not they carry news. Meta, Google and TikTok are anticipated to fall within scope. Consultation closed in December 2025, with draft legislation to follow.
6	**Continued ACCC focus on digital markets:** While the Government continues to evaluate a broad wave of digital law reforms, the ACCC continues to pursue digital platforms under current laws. The ACCC's 2026-27 enforcement priorities confirm its continued focus on "manipulative and false practices and unsafe consumer goods in digital markets" and "promoting competition in digital markets". In 2025, the ACCC secured a $55 million penalty against Google in relation to anti-competitive pre-installation understandings with Telstra and Optus, following admissions and an undertaking by Google. Current enforcement efforts include ongoing proceedings against Microsoft over subscription transparency and various misleading conduct cases against consumer-facing platforms such as Webjet and eHarmony.
7	**A new approach to digital platform disputes?** In its final report on the 5-year Digital Platform Services Inquiry, the ACCC reiterated prior recommendations for mandatory internal dispute resolution standards and an independent ombuds scheme for small business and consumer disputes with digital platforms. Australia's Telecommunications Industry Ombudsman claims it is "ready to take on the role of Communications Ombudsman … across telco and digital services" and the privacy regulator proposed expanding industry dispute resolution schemes, identifying digital platforms as a candidate sector.



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 YouFoodz**
  Alleging misleading or deceptive conduct in relation to subscription sign-up and cancellation practices.

- **ACCC v Microsoft**
  Alleging misleading or deceptive conduct in relation to subscription options and pricing for Microsoft 365 plans after integrating Copilot AI.

- **Epic/Google/Apple litigation and class actions**
  Following release of the lengthy judgments in 2025, the Epic Games 'misuse of market power' cases have moved to remedies hearings. Judgment expected by the end of the year.

- **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 action against Google**
  Alleging misuse of market power and unconscionable conduct in digital advertising, resulting in loss of revenue to publishers. Follows similar proceedings in the US, UK and Canada.

- **Dialogue Consulting v Instagram**
  Alleging withdrawal of access to products constituted misuse of market power, misleading conduct and unconscionable conduct. Three week hearing scheduled for Q3 in 2026.

AI	
1	**No broad AI-regulation for now:** Under the National AI Plan, AI risks will be regulated using existing laws and regulators. We won't see an "AI Act" in the short term, but the adequacy of our current laws for addressing new and emerging AI risks will continue to be reviewed and monitored. A 2025 Treasury review of AI and the Australian Consumer Law found it is broadly fit for purpose, and there are no proposals to prioritise AI services for designation under the proposed ex ante digital competition regime.
2	**A new AI Safety Institute** will provide regulatory and technical advice across government, informing regulatory interventions.
3	**Expect targeted regulatory activity** in response to new areas of concern. Agentic AI is on the radar of the ACCC and ASIC, and eSafety is monitoring AI "nudify" apps and AI companions.
4	**Continued push for AI governance:** Expect AI management frameworks and guidance (such as Australia's Voluntary AI Safety Standard and Guidance for AI Adoption) to inform the "reasonable steps" expected of organisations.
5	**No copyright exemption for data mining / AI training:** It has been confirmed that Australia is not considering a data mining or AI training exemption in the Copyright Act. Instead, the Productivity Commission called for a review of copyright and AI over three years – read more. In the meantime, the copyright and artificial intelligence reference group is engaging on topics including licensing arrangements, copyright in AI-generated materials, and low-cost enforcement for infringing AI outputs. Expect moves to unlock high-value datasets for AI training, flagged in the National AI Plan.
6	**Automated decisions:** Privacy laws requiring transparency around AI and computer-assisted decisions (and personal information used to make them) will come into force in December 2026. Read more.
7	**Technology at work:** NSW has new safety laws for digital work systems. The Victorian Government supported most recommendations from the Inquiry Into Workplace Surveillance. Last year's The Future of Work report made extensive recommendations. With recent calls from Government to elevate workers' voices in AI, and US litigation on AI job applicant screening, expect more on technology at work.

Key cases to watch

- **Getty Images v Stability AI**
  Filed in the UK and Stability AI was largely successful at first instance. Permission to appeal has been granted on the secondary copyright infringement claim and is expected to progress in 2026.
- **Kistler v Eightfold AI**
  A January 2026 US class action alleging that scraping of personal data and AI ranking and screening of job applicants didn't comply with credit and consumer reporting and unfair business practices laws.
- **Mobley v Workday**
  US "opt in" collective action alleging age discrimination in Workday's AI recommendation systems that score, sort, rank, or screen job applicants.

Privacy, Data and Cyber Security	
1	**A "modernised and clear" Privacy Act?** An initial tranche of privacy reforms passed in November 2024 deferred the majority of recommended reforms. Instead, the Productivity Commission recommended a major pivot to an "outcomes-based" duty to act "fair and reasonably", replacing the current prescriptive framework. The Government's response remains to be seen, as in the National AI Plan the Government said it is developing a "modernised and clear" Privacy Act. We will likely see some proposed reforms progressed in 2026, but a significant pivot would be a multi-year project.
2	**Serious invasion of privacy actions:** 2025 brought a new statutory tort, for serious invasions of privacy, not limited to Privacy Act breaches. In 2026, expect activists, private litigants, and employees to test the boundaries of the action, including through class actions and applications for interim injunctions.
3	**More civil penalties:** Australia has seen its first civil penalties under privacy laws (Australian Clinical Labs, $5.8 million) and under financial licensee obligations (FIIG Securities, $2.5 million) following data breaches. The penalty in Australian Clinical Labs was at the lower end of the permissible range, sounding a warning to business that serious privacy breaches could result in substantial penalties.
4	**New focus areas:** The OAIC will progress investigations into rental tech, connected cars, and tracking pixels.
5	**Children's Online Privacy Code** for social media, online communications, internet services, and others is being prepared, subject to 60 days of consultation and to be registered by 10 December 2026. Where possible, the code is expected to align with the UK's Age Appropriate Design Code and we expect it will supplement new online safety codes taking effect from 9 March 2026.
6	**Critical infrastructure risk management rules:** Proposed updates focus on nation state actors, interconnectedness, and supply chains. Key issues include foreign ownership and interference, insider threats, opaque supply chains, and emerging threat vectors such as AI and quantum computing.
7	**Cyber Incident Review Board** will conduct "no-fault" reviews of significant cyber security incidents to identify root causes and systemic issues.
8	**Smart devices:** New security standards commenced March 2026, requiring compliance statements from manufacturers and suppliers.
9	**Further "Horizon 2" cyber reforms?** Horizon 2 of the Australian Cyber Security Strategy spans 2026-2028, and key themes of a 2025 discussion paper included structural reforms to harmonise and simplify cyber regulation.

Key cases to watch

- **Optus, Medibank**
  Each facing regulatory prosecutions, class actions and representative complaints following major cyber incidents that give rise to issues relating to the intersection of data governance, privacy and cyber security.
- **ASIC v Fortnum**
  ASIC's third cyber security case against financial services licensees, this time involving attacks against Fortnum's adviser network.

Online Safety	
1	**Social media minimum age:** World-first laws requiring reasonable steps to prevent under 16s having social media accounts came into force December 2025. 2026 will see constitutional challenges, as well as monitoring and potentially enforcement activity – and administrative law challenges in response. An independent legislative review is required within 2 years, and eSafety has already launched a two-year study of how regime is working in practice.
2	**New codes to age-gate content:** Platforms, websites, telcos, search engines, and others will need to restrict access to age-inappropriate content under new "age-restricted media" codes – three are in effect, with six more applying from 9 March 2026.
3	**The international age of age assurance:** Australian, EU, and UK online safety regulators announced a trilateral cooperation group on age assurance, and the Global Online Safety Regulators Network released a position statement prioritising age assurance in online safety regulation. With no single approved or dominant approach to age assurance, we are already seeing concerns about accuracy, and children avoiding restrictions using VPNs or by migrating to other platforms that aren't captured by the restrictions.
4	**AI "nudify" apps and stalking tools:** The Government is working with industry on restricting abusive technology including AI "nudify" apps and undetectable online stalking tools.
5	**Digital Duty of Care:** The Australian Government is expected to progress digital duty of care legislation following a consultation via a public survey in December 2025.
6	**More reforms?** A Statutory Review of the Online Safety Act made 67 recommendations. The Government has not responded to most recommendations – which include expanded investigatory powers and regulatory tools, and a shift from a single eSafety Commissioner to a multi-member commission model.

Key cases to watch

- **Challenges to social media minimum age laws** in the High Court from both Reddit and the Digital Freedom Project. The cases will progress in parallel, with a further directions hearing in April 2026.
- **eSafety v X Corp**
  After a series of appeals, 2026 will see civil penalty proceedings for non-compliance with a 2023 transparency reporting notice on steps taken to combat child sexual exploitation and abuse material.
- **Raine v OpenAI**
  Filed in the US in August 2025, alleging that interactions with ChatGPT-4o contributed to a teenager's suicide.
- **Social media adolescent addiction**
  Multidistrict litigation in the US will continue with the first bellwether case to go to trial in June 2026.

Telco and Connectivity	
1	**New registration scheme:** An Enhancing Consumer Safeguards bill may pass in the first half of 2026, introducing a carriage service provider registration scheme impacting companies that provide or arrange connectivity – this could include IoT and smart devices, vehicles and infrastructure, as well as remote site operators (eg mining and construction), and service resellers.
2	**New enforcement powers:** The Enhancing Consumer Safeguards bill also includes bigger penalties and more regulator powers – including to directly enforce codes and standards.
3	**Universal mobile and direct-to-device satellite:** New laws may pass mandating baseline mobile coverage across Australia, supported by terrestrial networks and direct-to-device LEO satellite.
4	**Further telco reform:** Hot-button issues include consumer protection, network reliability and security (particularly emergency services), and universal services.
5	**Data centre principles:** The Government is working with States on draft national data centre principles aimed at managing energy and water impacts of data centres, without discouraging investment. We expect principles to set benchmarks (eg renewable energy and efficient cooling technologies) to qualify for streamlined development approvals. It remains to be seen whether Australia will follow the US proposal to require data centres to meet their own electricity needs. Monitor our Data Centre Hub for updates.
6	**Data centre inquiry:** Driven by the AI race, data sovereignty and geopolitics and supported by the National AI Strategy, there is unprecedented demand for data centres in Australia. However, the exponential growth required to meet this demand brings its own challenges and the NSW Legislative Council has launched an inquiry into data centres in the State. Key areas of focus for the inquiry include: the planning frameworks enabling data centre developments; electricity demands, grid impacts and impacts on emissions reduction targets; water usage; and impacts on the local environment and community. See our article for more details.

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
Consultant
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

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

Risk Advisory

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

Rachael Falk
Partner, Cyber, Risk Advisory
T +61 2 9258 6405
rachael.falk
@ashurst.com

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

For Trending Topics and Insights from Ashurst, visit https://www.ashurst.com/en/insights/content-hubs/

Ashurst

ashurst.com

Design Ref: R016734 Mar 26