

What's Ahead: 2024 Digital Economy in Australia

Digital platforms, online content providers and other businesses active in the digital economy face an increasingly complex and evolving regulatory and legal landscape in Australia. With privacy and data regulation, AI, intellectual property, online safety, competition and consumer issues increasingly intertwined in the digital sphere, staying ahead of the curve requires an integrated, multi-disciplinary approach, enabling future-proof strategies that are consistent across legal areas. Here is our take on key themes this year:

1. **Ongoing intensive rolling regulatory reform, which will disrupt how businesses operate:** On the back of an ambitious reform agenda in 2023, in 2024 we will see the implementation of legislation and further consultation on new regulations impacting the digital economy. Digital platform consumer measures (including scams) and competition rules, significant amendments to the Privacy Act, regulation of AI, and misinformation / disinformation are among the likely key reforms with significant implications for businesses active in the digital economy.
2. **More aggressive enforcement and higher penalties:** by the Australian Competition and Consumer Commission (**ACCC**), Office of the Australian Information Commissioner (**OAIC**), the Australian Communications and Media Authority (**ACMA**) and eSafety Commissioner. Armed with greater funding, resources and expertise, and the ability to seek massive penalties, we will see more investigations, pursuit of novel theories of harm and higher penalties.
3. **More private actions:** Recent years have seen an uptick in private proceedings, including class actions, alleging breaches of competition, consumer and privacy laws. This year, Epic's proceedings against Apple and Google (and related class actions) regarding mobile app distribution will be heard, and data breach class actions against Optus, Medibank and Latitude continue to progress at pace. There is an increase in litigation worldwide in relation to infringement of copyright in the training of AI tools.
4. **Greater co-ordination between regulators:** An increasing intersection of competition, consumer protection, privacy, online safety and data issues is driving greater co-operation between regulators, in Australia and abroad. The Digital Platform Regulators Forum, formed by the ACCC, the ACMA, eSafety and the OAIC, is prioritising assessment of generative AI, improving transparency and increasing collaboration and capacity building.
5. **Intensified scrutiny of AI including algorithms, automated decision making and generative AI:** While we await further regulation, we expect greater scrutiny of AI under existing laws. It is important that businesses understand exactly where and why AI or automated decision making is used in their organisations and supply chains.

What's Ahead: 2024 Digital Economy

AI

- AI-specific regulation:** The Government released its [interim response](#) to the AI consultation, signalling a temporary advisory body to develop laws to introduce mandatory safeguards for "high risk" AI (including a possible voluntary labelling scheme for AI generated content) and tasking the National AI Centre to develop a voluntary risk-based AI Safety Standard.
- New AI Management System standard:** The new standard [ISO/IEC 42001:2023](#) is expected to be adopted as an Australia Standard.
- Global guidelines for secure AI system development:** [Guidelines for secure AI system development](#) released in November 2023 by international cyber agencies (including Australia) require providers to take responsibility for the security outcomes of users further down the supply chain, a philosophy likely to flow through to regulation.
- Copyright and AI reference group:** To be established in 2024 as a standing mechanism for stakeholders to engage with the Government regarding copyright issues associated with the use of AI.

Privacy and Data

- Reforms to Privacy Act:** 2024 will see consultation and draft legislation now that the Government has published its [response to the Privacy Act Review Report](#). Proposed reforms include extending regulator powers and information security requirements, and "in principle" agreement on data breach notification timeframes, a new "fair and reasonable" test, and stricter direct marketing and advertising rules.
- Automated decision making:** will be an early focus of privacy reforms, with additional reforms to government automated decisions following the Royal Commission into Robodebt.
- New Privacy Commissioner:** The OAIC has returned to having three dedicated commissioners. Incoming Privacy Commissioner, Carly Kind, is expected bring experience of British and European strategies and experience in the intersection of technology policy and human rights.
- Digital ID:** Australia remains committed to a whole-of-economy interoperable Digital ID. The [Senate report](#) into the Digital ID Bill is due 28 February, with the goal of a national scheme up and running by July. See our publication [A deeper dive into Australia's Digital ID Bill](#).
- The Consumer Data Right (CDR):** will be [expanded to non-bank lending](#) with draft rules expected in 2024. While Australia's expansion of the CDR has slowed, the government's goal for a whole-of-economy CDR remains.
- Focus on dark patterns:** The Global Privacy Enforcement Network of privacy regulators conducted a review of deceptive design in websites and apps. Expect a more active regulatory stance, investigations and potentially enforcement and law reform in 2024. Dark patterns is also a focus area of potential reforms to the CDR, and ACCC scrutiny: see 'Competition and Consumer Protection' below.

Online Safety and Misinformation

- Increased regulatory action on Online Safety:** The Government opened consultation to strengthen the Basic Online Safety Expectations – to address gaps, emerging harms, and further clarify the government's expectations of industry. Issues canvassed include services using generative AI to create unlawful or harmful material, and a new expectation that industry consider the best interests of children, potentially including age assurance mechanisms.
- More administrative review actions?** The eSafety Commissioner has adopted a close to zero tolerance stance on online safety standards – we will see more aggressive enforcement, which may result in more litigation as industry looks to have decisions reviewed.
- Revised Misinformation Bill:** After 2023's consultation, the Government is considering changes including around definitions, transparency, accountability, religious freedoms and ensuring it is practically workable for digital platforms.
- Decline of co-regulation:** ACMA has signalled doubt about the ongoing viability of the co-regulatory approach with industry adopted since the 1990's especially in relation to media on tech platforms. It is likely they will adopt a more directive policy and regulatory stance in the year to come.
- Privacy law/ secrecy legislation:** The government will continue to pursue regulatory approaches to limit "harmful" information in the media and we can expect further secrecy legislation and privacy law amendments that will significantly affect all publishers, particular a right of action for invasion of privacy supplanting defamation actions following the UK trend. This may become a significant impost on major publishers and platforms.

Cases to watch

New York Times v OpenAI: filed in the US in December 2023, alleging that the training of Open AI infringed New York Times copyright.

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.

Optus, Medibank and Latitude: each facing representative complaints with the OAIC as well as class actions, following major cyber incidents. Medibank is also facing a shareholder class action for its cyber incident.

OAIC v Meta: following the court's decision on extraterritorial reach of the Privacy Act, in late 2023 Meta filed its defence to the OAIC's allegation that Meta breached the APPs in relation to the Cambridge Analytica incident.

eSafety v X Corp: alleging failure to comply with a transparency notice under the Online Safety Act. X did not pay an infringement notice, and has sought judicial review of it.

What's Ahead: 2024 Digital Economy

Cyber security

- 1. New cyber laws and critical infrastructure reform:** Following the release of [Australia's cyber strategy](#), the Government is consulting on new cyber security laws including a mandatory security standard for IoT devices and changes to the Security of Critical Infrastructure Act 2018. Submissions close 1 March 2024: [Cyber Security Legislative Reforms](#).
- 2. 2023-2030 Australian Cyber Security Strategy:** released 22 November 2023 contemplates further law reform and a raft of non-legislative initiatives. Read more in our publication [Australia cyber strategy – a bold regulatory reform agenda](#).
- 3. Focus on Board and Director responsibility for cyber risk management:** A [speech](#) by ASIC Chair Joe Longo highlights that ASIC expects cyber risk management to be a top priority for all boards. This includes the management of cyber risk arising from reliance on third-party providers. ASIC has indicated its intention to take action against directors who fail to adopt adequate measures on the basis that they have not exercised care and diligence, as required under section 180 of the *Corporations Act 2001* (Cth).

Competition and Consumer Protection

- 1. Ex Ante Digital Platform Regulation:** The Government [announced](#) its in principle support of the ACCC's recommendations to introduce digital platform consumer measures (see 2, 4 & 5 below) and mandatory service-specific codes for designated digital platforms containing targeted competition obligations. Treasury will work on framework design, informed by further consultation and international developments.
- 2. Scams Code Framework:** Following the establishment of the National Anti-Scam Centre, the Government has committed to introduce industry codes to combat scams, with an initial focus on banks, digital communications platforms and telecommunications providers. [Consultation](#) on a proposed framework is underway. This is a priority area, given the huge losses Australians incur to scammers ([\\$3.1 billion in 2022](#)).
- 3. Merger Reform:** As part of the [Competition Review](#) being undertaken by the Competition Taskforce, an overhaul of Australia's merger control regime is under [consideration](#). Major changes to the merger control process and substantive test proposed by the ACCC are among the proposed options for reform. The Competition Review is also looking at **non-compete clauses**, with a consultation paper expected in early 2024.
- 4. Unfair Trading Practices:** The outcome of [consultation](#) on a proposed unfair trading practices prohibition is expected this year. Although the [proposal contemplated economy-wide application](#), it was directed at many online practices, including dark patterns, hard-to-cancel subscriptions and click wrap consents for tracking and data collection.
- 5. Dispute Resolution:** The Government has called for digital platforms to develop voluntary internal dispute resolution standards by July 2024, and has signalled further work on external dispute resolution requirements.
- 6. "Super Complaints":** A designated complaints function for the ACCC will likely be introduced this year, enabling designated consumer and small business advocates to raise significant or systemic issues and have them prioritised by the ACCC, modelled on the UK regime.
- 7. News Media Bargaining Code:** Government [will](#) adopt all [recommendations](#) coming out of Treasury's review of the code, but as yet, no platform has been designated.
- 8. ACCC Digital Platform Services Inquiry (DPSI):** The [inquiry](#) continues with the 8th interim report – examining [data broker services](#) - due on 31 March. There are two 6-month phases left, with a final report due to Treasury by 31 March 2025.
- 9. Continued scrutiny by the Digital Platforms Unit:** The specialist unit is investigating Apple's restriction of third-party access to NFC technology, and Google's ad tech business, and further investigations are likely. We expect focus on expanding ecosystems including through M&A, self-preferencing, restrictions on interoperability, fair dealings with small businesses and consumers, dark patterns, contextual advertising and data collection following the demise of third-party cookies, scams, hard-to-cancel subscriptions and fake reviews.

Cases to watch

ACCC v Meta: alleging false, misleading or deceptive conduct by publishing scam advertisements promoting cryptocurrency investment schemes featuring prominent Australian public figures.

ACCC v eHarmony: alleging false, misleading or deceptive conduct in relation to membership services, including autorenewal and early cancellation.

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. Hearing in March-July 2024.

Sony Interactive class action: filed in December 2023, alleging competition law breaches.

Hamilton v Meta and Google (Appeal): class action accusing Meta and Google of breaching competition law (cartel conduct, anti-competitive agreements or concerned practices) by banning cryptocurrency ads.

Dialogue Consulting v Instagram: alleging withdrawal of access to products contravened misuse of market power, misleading conduct and unconscionable conduct. Hearing date yet to be set.

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

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

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

Risk Advisory



John Macpherson

Partner, Head of Cyber Response
T +61 2 9258 6479
john.macpherson@ashurst.com



Leon Franklin

Director, Regulatory risk, engagement & privacy
T +61 2 9258 6021
leon.franklin@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

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

