the global voice of the legal profession

IBA Intellectual Property, Communications and Technology Law Committee

# Digital Regulations in the Metaverse Era

# AUSTRALIA

Regional Coordinators:
Angela Flannery *Quay Law Partners, Sydney*
Yoshifumi Onodera *Mori Hamada & Matsumoto, Tokyo*

# Data

Angela Flannery *Quay Law Partners, Sydney*

## Q 1. Does Australia have any specific data or privacy laws that deal with the metaverse?

Australia currently does not have any specific laws regulating the use of data (whether personal or non-personal) in the metaverse. There are, however, many generally applicable laws relating to data that will apply to metaverse activities, including:

- in relation to the use of personal information, the Privacy Act 1988 (Cth) ('Privacy Act'), which is a federal law regulating the collection, use, disclosure and retention of personal information that applies to both public and private sector entities (including for-profit and not-for-profit entities);
- in relation to the use of data that is protected by intellectual property rights, there are a number of applicable laws, for example, the Copyright Act 1968 (Cth) and the Trade Marks Act 1995 (Cth).

## Q 2. Does the Australian Privacy Act apply to the metaverse?

Australia's Privacy Act became law in 1988. In 2019, the Australian government announced that the Act would be reformed to make it fit for purpose in the digital age. That reform process has progressed slowly and, by early 2024, no major changes to the Privacy Act have been implemented. The Australian government has announced the principles that it intends to implement in the reformed Privacy Act, and it is expected that legislation will be passed during 2024.

The Privacy Act regime, in its current form and as it is to be reformed, extends to the metaverse, given the jurisdictional application of the Act. The following discussion looks at the jurisdictional nexus and three key areas of regulation, namely, data minimisation, the use of personal information for marketing and targeting and the collection of personal information from children.

## Q 3. Is there a jurisdictional nexus for the application of the Privacy Act to the metaverse?

This will depend on the specific circumstances of each individual case. The jurisdictional reach of the Privacy Act has been the subject of significant scrutiny in recent times, with Meta challenging the jurisdiction of the Australian Information Commissioner ('Commissioner') who, together with the Office of the Australian Information Commissioner, is the regulator for the Privacy Act. The Commissioner commenced proceedings against Facebook Inc, a United States-domiciled company in relation to the Cambridge Analytica scandal. Meta was unsuccessful before the Australian courts in regard to its arguments that the Privacy Act did not apply to Facebook Inc.[1]

The Privacy Act will apply to acts or practices outside Australia with an 'Australian link'. Under section 5B of the Privacy Act (noting that it has been amended since the time of the Cambridge Analytica scandal), an Australian link will be established for an entity incorporated outside Australia where it carries on business in Australia. Based on the decision in the Meta case, this criterion will be satisfied even if the only activity occurring in Australia is installing and removing cookies from devices used in Australia (for the purposes of targeted advertising) or the management of application programming interfaces (APIs) that may be used for collecting and sharing the personal information of individuals located

1 Meta was refused leave to appeal to the High Court against the Federal Court of Australia's determination that the Commissioner had jurisdiction, see *Facebook Inc v Australian Information Commissioner* [2023] HCATrans 22 (7 March 2023).

in Australia. Therefore, businesses providing metaverse services to Australian users should assume that they are subject to the Privacy Act, even if the business does not maintain a physical presence in Australia.

## Q 4. What are the key provisions in the Australian Privacy Act that would apply to the design and implementation of metaverse platforms?

The primary compliance requirements under the Privacy Act are set out in the Australian Privacy Principles (APPs) that form Schedule 1 to the Privacy Act. Key obligations under the Privacy Act that impact the metaverse include:

- data minimisation: Pursuant to APP 3, a private sector entity must only collect personal information that is reasonably necessary for one or more of its functions and activities. If the personal information falls within a category of 'sensitive information', such as health information or biometric data, used for identification purposes, then, in addition, it may only be collected if the consent of the relevant individual is obtained;
- use of personal information for marketing or targeting: APP 7 regulates the use of personal information for targeted marketing, which extends to the online environment, although there has been limited enforcement in this regard. This situation is likely to change when the Privacy Act reforms are introduced in 2024, which propose greater restrictions in this area. For example, the proposed reforms aim to provide to provide individuals with an unqualified right to opt out of their personal information being used for targeted online advertising. In addition, the proposed reforms include that that all targeting must be fair and reasonable, with targeting based on sensitive information, such as health information, religion or political beliefs, being banned entirely;
- children: There are currently no special protections for children (defined as individuals under 18 years) under the Privacy Act. Where consent is required for personal information collection, the Act does not define an age of consent for children. The Commissioner applies a rule that individuals aged 15 and over have the capacity to provide consent. While the rules in relation to the capacity to provide consent will not be changed under the proposed 2024 Privacy Act reforms, regulated entities will need to have regard to the best interests of the child in collecting and using their personal information and a Children's Online Privacy Code will be introduced. The ability to use personal information of children for targeting will be strictly curtailed.

As the proposed reforms to the Privacy Act will expand the scope of regulated personal information, particularly to make clear that it includes certain technical information, businesses operating in the metaverse will need to ensure strict compliance with the requirements of the Privacy Act listed above, among others.

## Q 5. What action could be taken if a metaverse business breaches the Privacy Act?

In 2022, the Privacy Act was amended to bring the penalties for substantive breaches of the Privacy Act into line with the penalties that apply for breaches of Australia's primary consumer protection legislation, the Australian Consumer Law. Liability for a breach by a body corporate results in a maximum monetary penalty of of AU$50m, three times the benefit the body corporate receives from the breach or, where such benefit cannot be determined, 30 per cent of the turnover of the body corporate from its Australian business.

As at early 2024, individuals do not have any rights to directly take action for a breach of the Privacy Act. If an individual wishes to seek compensation for breaches of their privacy, they must either take action under another law, such as for breach of the misleading and deceptive conduct provisions in the Australian Consumer Law, or ask the Commissioner to investigate the breach and make a determination for compensation. This situation will change when the reforms to the Privacy Act are introduced during 2024. Those reforms will provide for a direct right of action for individuals where their privacy has been interfered with through a breach of the Privacy Act. Australia is very active in the area of class action litigation: in future, metaverse businesses that breach the Privacy Act may find that they face very high penalties, not only from action taken by the Commissioner, but also through class action litigation.

# Human rights, accessibility and digital ethics

## Q 1. Are there any specific Australian human rights, accessibility or digital ethics laws or regulations that would apply to the metaverse?

There are no specific laws in these areas that apply only to the metaverse, but there are numerous Australian laws that regulate human rights, accessibility and digital ethics, many of which will impact the metaverse. This section considers the following, and the implications of these laws (and potential laws) for the metaverse:

- the Online Safety Act 2021 (Cth);
- proposed laws to regulate mis- and disinformation; and
- the rules aimed at preventing online scam activity.

## Q 2. How does Australia's Online Safety Act apply to the metaverse?

Australia's Online Safety Act has few equivalents in other jurisdictions, although the UK's Online Safety Act, which became law in October 2023, broadly regulates the same areas. In fact, in early 2024, Australia and the UK signed a Memorandum of Understanding to cooperate to support safer and more positive online experiences.

The primary purpose of the Act is to provide for the online protection of vulnerable members of the community, particularly children. Broadly speaking, the Online Safety Act regulates cyberbullying and harmful online material such as hate speech and image-based abuse. The Act applies to a range of platforms and online services that are accessible in Australia and it will capture metaverse businesses in most cases.

Online safety is a hot topic politically in Australia, with regulation in this area likely to continue to expand.

## Q 3. How could the eSafety Commissioner, the regulator for the Online Safety Act, take action in relation to the metaverse?

The eSafety Commissioner is the regulator responsible for enforcement of the Online Safety Act and is able to investigate complaints in relation to online:

- adult cyberabuse;
- cyberbullying of children (which extends beyond bullying on social media);
- image-based abuse; and
- illegal and restricted content (broadly speaking, comprising pornographic or highly violent material).

The eSafety Commissioner has powers to require that material in the categories listed above is removed from online sites in particular circumstances if a complaint is found to be substantiated, or in the case of abhorrent violent content, to require that material to be blocked in crisis situations.

## Q 4. Would the Online Safety Act's 'Basic Online Safety Expectations' apply to metaverse businesses?

Yes. The Online Safety Act establishes 'Basic Online Safety Expectations' (BOSEs) that regulated providers should comply with to assist in ensuring that online services are safe to use. While there are no prescribed penalties for breaches of these expectations,[2] the BOSEs create minimum 'safety by design' thresholds for platforms.

The Online Safety Act also provides for the development of codes or, where necessary, mandatory standards to apply to illegal and restricted content. A failure to comply with those codes or standards carries civil penalties. Therefore, metaverse businesses falling within the scope of the regime have strong incentives to comply.

## Q 5. Can the eSafety Commissioner ask metaverse businesses for information?

Yes. The eSafety Commissioner has powers to require online service providers to supply information to the eSafety Commissioner as to how those providers are combatting harms. The eSafety Commissioner regularly uses this power. For example, in March 2024, the eSafety Commissioner issued notices to Google, Meta, X, WhatsApp, Telegram and Reddit, requiring each of those platforms to report as to what steps they are taking to combat terrorist and violent extremist material on their sites.[3]

## Q 6. What Australian mis- and disinformation regulation would apply to the metaverse?

As of April 2024, Australia does not have any laws that specifically regulate online mis- and disinformation. DIGI, the digital platforms lobby group in Australia, has implemented a voluntary Australian Code of Practice on Disinformation and Misinformation.[4] That Code is of limited efficacy, as its scope is quite limited and of course it is voluntary. Only a small number of digital services providers have agreed to comply with the Code, although it does cover most large platforms, for example, Google, Meta and TikTok. Metaverse businesses may in future face pressure to sign up to the Code.

## Q 7. Are there any new laws on mis- and disinformation that are in the pipeline in Australia that might apply to the metaverse?

Yes. In mid-2023, the government commenced a consultation process for new legislation that would grant powers to Australia's communications sector regulator, the Australian Communications and Media Authority (ACMA), to combat online mis- and disinformation. Under the proposed law, the ACMA would:

- have powers to compel the provision of information from digital platforms and require record keeping by those platforms in relation to mis- and disinformation;
- be able to require the development by the sector of a code of practice to combat mis- and disinformation, which ACMA could register and enforce; and
- if any code of practice was unsuccessful in combatting online mis- and disinformation, be empowered to develop and enforce an industry standard.

2 While there are no penalties for breaches, there are penalties for failures to report to the eSafety Commissioner in relation to compliance.

3 The eSafety Commissioner's media release announcing the issuance of these notices is here: www.esafety.gov.au/newsroom/media-releases/tech-companies-grilled-on-how-they-are-tackling-terror-and-violent-extremism.

4 The Code is available here: https://digi.org.au/disinformation-code/.

The government's proposal met with significant resistance due to concerns that the proposed new law would unduly inhibit freedom of speech. The government is expected to introduce a revised legislative proposal during the course of 2024. Assuming the revised proposal addresses the concerns raised by stakeholders regarding the initial scheme, it is likely that specific regulation of online mis- and disinformation will commence by the end of 2024 or early 2025. This will apply to metaverse platforms and services.

## Q 8. Is there any regulation of dating in the metaverse in Australia?

Yes. In July 2024, many of the larger online dating companies, such as Match Group, Bumble and Grindr, agreed to a voluntary code regulating matters such as the implementation of systems to detect harm and taking action to oust users that violate their online safety policies. There would be significant political and community pressure for any metaverse businesses that offered dating services to sign up to this code.

## Q 9. Would Australia's online scam prevention rules apply in the metaverse?

While there are only limited specific laws regarding online scams in Australia, those laws are used in relation to all types of businesses with an online presence and would apply to metaverse businesses.

A key concern in terms of ethics and the protection of individuals in regard to their online engagement, which will have implications for the metaverse, is the proliferation of online scam activities, particularly through paid advertising on digital platforms. In 2022, more than AU$3bn was lost by Australians (often the most vulnerable in the community, such as the elderly), with a significant number of the scams perpetrated over the internet and via social media sites.[5]

While the three federal regulators with the most significant enforcement role in regard to combatting scams, the Australian Competition and Consumer Commission (ACCC), the Australian Securities and Investments Commission (ASIC) and the ACMA, have all worked diligently to enforce existing laws to combat online scams, the Australian government has signalled that more needs to be done.

## Q 10. Are any new laws proposed that will regulate scams in the metaverse?

In late 2023, the government commenced consultation on a new legislative framework for the regulation of scam activities. The proposed framework will apply across the economy, including in the metaverse, imposing a minimum set of requirements on regulated businesses to respond to scam activity. In addition, there will be sector-specific codes and standards that impose additional obligations, targeted at the relevant sector. The ACMA will have responsibility for the implementation of codes and standards for digital communications platforms, to be broadly defined and likely to include metaverse services. While the government has indicated that social media sites are the digital communications platforms of most concern, metaverse providers will need to rigorously police scam activities against scam activities when the new framework, and the new codes and standards, take effect.

5 The ACCC publishes data on scam activity on an annual basis. The reports are available here: www.accc.gov.au/about-us/publications/serial-publications/targeting-scams-reports-on-scams-activity.

# Competition law

## Q 1. How is competition in the metaverse regulated in Australia?

Australia currently does not have any specific laws that regulate competition in the metaverse. However, ever since Australia's competition regulator, the ACCC, undertook its groundbreaking inquiry into digital platforms in 2017–2019 (the 'Digital Platforms Inquiry'), it has pushed for specific regulation of digital platforms, which would apply to the metaverse. The proposals put forward by the ACCC, which are (as of April 2024) being considered by the Australian government, are discussed in this section.

## Q 2. Will Australia's proposed merger law reform impact metaverse businesses?

Yes. In the second half of 2023, the Australian government announced the establishment of a Competition Taskforce within the Australian Treasury to consider a range of reforms to Australia's competition laws.

The first area that the Taskforce has tackled is merger law reform. At the current time, Australia does not have a mandatory merger notification regime. Instead, anticompetitive mergers are prohibited under the Competition and Consumer Act 2010 (Cth) (CCA). If parties to a merger seek certainty that the ACCC will not pursue them for breach of the CCA, they may seek an informal clearance from the ACCC under processes that it has established for this purpose, outside the scope of the CCA. If the ACCC notifies the parties under that informal clearance regime it will not take action to block a merger, provided full disclosure has been made by the parties, this in a practical sense allows the merger to proceed. The CCA contains a formal authorisation process for mergers. Where an authorisation is granted under that regime, no challenge may be made to the merger, either by the ACCC or by third parties.

## Q 3. How will those merger laws apply to metaverse businesses?

The proposed reforms to the merger regime proposed by the Competition Taskforce contemplate the possibility of a mandatory merger notification regime. This has been championed by the ACCC in part because of concerns regarding mergers in the digital platforms sector, particularly so-called 'killer acquisitions', where a large digital platform acquires a nascent competitor, largely to stop the growth of that competitor and to stop it becoming a serious challenger in the future. This is a concern that is also very prevalent for other competition regulators, including in Europe. Another concern of the ACCC (shared by the Australian government) is in the area of vertical or conglomerate mergers, where digital platforms have acquired businesses in adjacent markets, leading to anticompetitive impacts due to the foreclosure of competition. For example, expansion into adjacent markets may provide access to additional key inputs, such as data and data sources or additional users, heightening barriers to entry for other competitors.

If Australia does move to a mandatory merger notification regime, which seems a probable outcome of the current Competition Taskforce review, the notification threshold may be fairly low and businesses operating in the metaverse are likely to have their mergers closely examined by the ACCC.

## Q 4. Will metaverse businesses fall within the contemplated Australian digital platform-specific competition laws?

From the ACCC's perspective, 'digital platforms' encompass online services that are typically multi-sided and that provide services to different groups of users, meaning metaverse services will inevitably fall within that definition. The ACCC first suggested the potential for direct competition regulation targeted at digital platforms in the final report resulting from its

Digital Platforms Inquiry. The ACCC repeated its call for such a regulation in reports it released in September 2022 and September 2023, in regard to its separate Digital Platform Services Inquiry.

## Q 5. What are some of the key provisions in the proposed digital platform-specific specific laws that might impact the metaverse?

The digital platform-specific regulatory reforms the ACCC has recommended share some similarities to the EU's Digital Markets Act (DMA) and reflect the same concerns that led to the enactment of the DMA. The ACCC's recommendations, which would apply to metaverse businesses if designated, are:[6]

- that a new power is given to the ACCC to make mandatory codes for specific digital platform services based on principles set out in the CCA. This would allow the ACCC to make codes that would apply, in each specific case, to only one identified digital platform and that regulated only the conduct of concern in relation to that platform;
- the mandatory codes would be able to address each of the following areas, depending on the platform to which the code applied:
  - anticompetitive self-preferencing;
  - anticompetitive tying;
  - exclusive pre-installation and default agreements that hinder competition;
  - impediments to consumer switching;
  - impediments to interoperability;
  - data-related barriers to entry and expansion, where privacy impacts can be managed;
  - a lack of transparency;
  - unfair dealings with business users; and
  - exclusivity and price parity clauses in contracts with business users.

A code could only be applied to a platform if it was designated, meaning that a finding would have to be made that the platform had both the incentive and ability to harm competition. If the proposed regime was adopted, given the likely designation criteria, the regime would apply to larger metaverse platforms. The ACCC suggests that designation should be determined in reference to quantitative or qualitative criteria, or a combination of both. The ACCC's proposed criteria are:

- quantitative criteria would be based on monthly active users and the relevant platform's revenue (either in Australia or globally); and
- qualitative criteria would be based on characteristics such as market power, the number of digital platform services that the platform operates and/or whether the platform has an important intermediary function.

It is likely that, at a future point in time, one or more metaverse platforms would satisfy either or both of these criteria.

The Australian government has shown only lukewarm support for the ACCC proposals. In December 2023, the government announced that it supported the reforms in principle and would direct the Treasury to develop the proposed legislative model, although further consultation would be required as that model was developed. As of April 2024, no legislative reform has been progressed and, therefore, at least in the short term, metaverse platforms may escape the application of DMA-style regulation in Australia.

6 The ACCC's full report setting out these recommendations is available here: www.accc.gov.au/inquiries-and-consultations/digital-platform-services-inquiry-2020-25/september-2022-interim-report.