Digital Platform Regulators Forum

Examination of technology: Immersive technologies

Working paper

September 2025

Important notice
This document has been prepared by the ACCC, ACMA, eSafety Commissioner and OAIC in their capacity as members of the Digital Platform Regulators Forum (**member regulator**). The information in this publication is for general guidance only. It does not constitute legal or other professional advice, and should not be relied on as a statement of the law in any jurisdiction. Because it is intended only as a general guide, it may contain generalisations. You should obtain professional advice if you have any specific concern.

The member regulators have made every reasonable effort to provide current and accurate information, but do not make any guarantees regarding the accuracy, currency or completeness of that information.

Parties who wish to re-publish or otherwise use the information in this publication must check this information for currency and accuracy prior to publication. This should be done prior to each publication edition, as member regulator guidance and relevant transitional legislation frequently change. Any queries parties have should be addressed to the dpreg@acma.gov.au.

Contents

1. Executive Summary

This working paper examines immersive technologies – also known as extended reality (XR) – which enable users to experience and interact in three dimensions with digital content in ways that look, sound and feel almost real. It is the fourth public paper released by the Digital Platform Regulators Forum (DP-REG) as part of its ongoing work to understand digital platform technologies and their implications for the regulatory roles of each member. The paper explores how immersive technologies may affect the media and information environment, privacy, online safety, consumer protection and competition within the digital platform context.

Use of immersive technologies has grown in recent years. While there are uncertainties around how these technologies will continue to be developed, this trend appears likely to continue, as diverse groups adopt these tools for entertainment, work, and everyday tasks. These technologies offer benefits across multiple industries – such as gaming, entertainment and retail – and may also enhance educational resources, improve digital literacy, and improve accessibility.

At the same time, immersive technologies raise specific concerns within each DP-REG members' area of responsibility, and may exacerbate existing risks and harms that each member is working to address in other areas of the digital economy. For example:

- **OAIC:** Immersive technologies are likely to heighten privacy risks through the increased collection, use, and disclosure of personal and sensitive information.
- **ACCC:** These technologies may introduce new avenues through which consumers may be harmed, including by scams or other manipulative conduct, and this conduct may be exacerbated by the extent and sensitive nature of data collected to supply immersive products and services. Competition issues may also arise at different levels of the XR supply chain, which may be driven by potentially significant barriers to entry and expansion, and the presence of large firms that supply related digital platform services.
- **ACMA:** Immersive technologies may increase the risk of online gambling harm and make it harder for users to assess the integrity and authenticity of information – increasing the impacts of disinformation.
- **eSafety:** The hyperrealism and ephemeral nature of experiences afforded by immersive technologies may amplify both existing and emerging online safety harms.

Some risks cut across each DP-REG member's distinct remit. For example, the potential for intensive collection of personal and possibly sensitive data[1], may contribute to people experiencing different harms in immersive environments that are each relevant to the responsibilities of a DP-REG member.

As immersive technologies are integrated with other emerging technologies, harms associated with each may also converge. For example, generative artificial intelligence (AI) could enable the creation and sharing of lifelike intimate content or immersive experiences without the consent of the people represented, or be used to manipulate users in immersive environments.

Consumer, competition, privacy, online safety and media laws or regulations that currently apply to platforms across the digital economy can address potential harms associated with immersive technologies, where those frameworks apply.

Proposed reforms the Australian Government is currently considering could also improve or strengthen regulatory responses to the potential harms posed by immersive technologies. The Government is considering law reform in relation to competition and online safety that may provide support to strengthen protections against these harms.[2] This is in addition to legislation passed in 2024 to enhance privacy protections, and in 2025 to enhance protections from scams, across the economy.[3]

This working paper is intended to complement and inform broader policy discussions about immersive technologies.

2. Background

This paper supports DP-REG's 2024-26 strategic priorities, which include 'understanding, assessing and responding to the benefits, risks and harms of technology'.[4] It also contributes to a deeper shared understanding of emerging technologies and enhances collaboration and capability across DP-REG members. This will support the future work of both DP-REG and its individual members.

Recent DP-REG working papers examined multimodal foundation models (MFMs) and large language models (LLMs), both of which are types of generative AI.

This paper focuses on immersive technologies, which are increasingly being developed and supplied in Australia and around the world. These technologies could bring significant benefits for individuals, businesses and industry, but may also heighten risks to individuals online. The paper examines the potential implications of immersive technologies for consumer protection, competition, the media and information environment, privacy, and online safety. It is also intended to provide background and context to support broader government work on immersive technologies.

3. Key insight questions

3.1 What are immersive technologies and how do they work?

What are immersive technologies?

Immersive technologies enable users to experience and interact with digital content in 3D, in ways that look, sound and feel almost real.[5] These technologies exist on a continuum from low to high immersion.[6] They also offer varying levels of interaction, both with the medium itself and between users.[7]

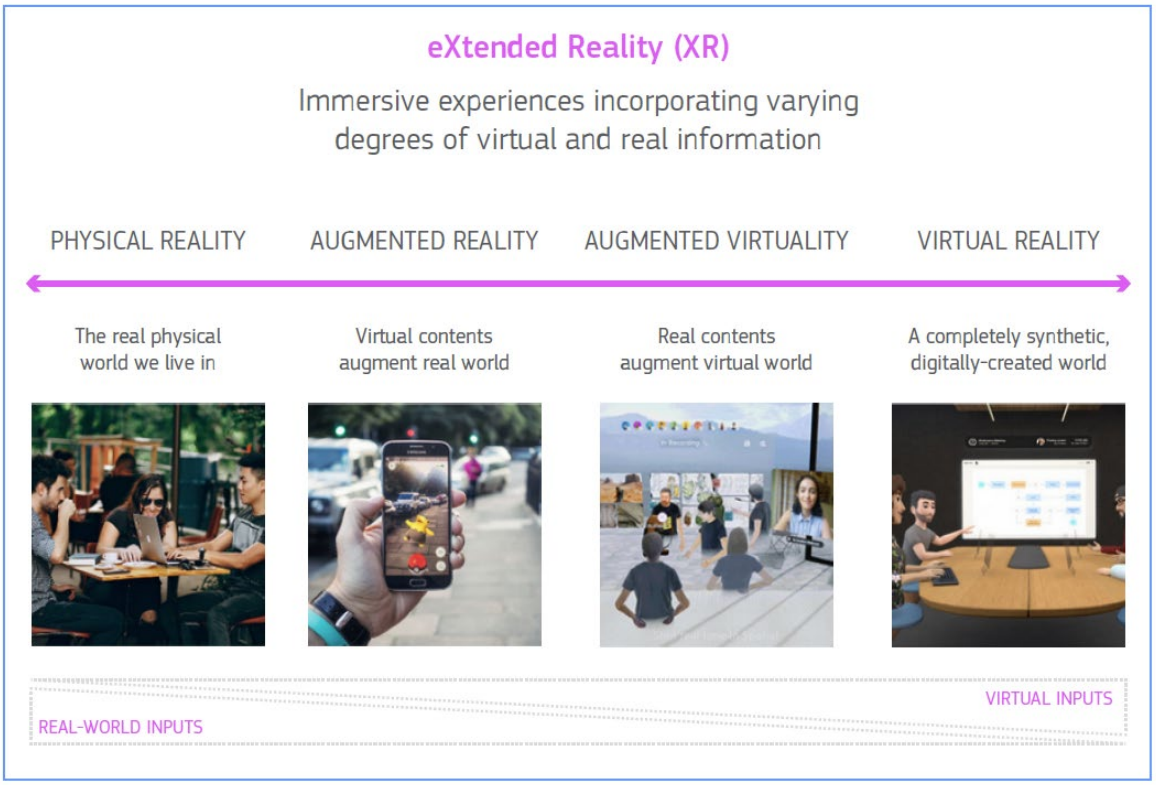
Immersive technologies include devices, software applications and services that use virtual reality (VR), mixed reality (MR), augmented reality (AR) and haptic feedback devices that mimic the sensation of touch – or some combination of these elements.[8] Haptic feedback devices are a core technology to extend immersive experiences. Other modalities such as smell and temperature could also be used to augment immersive experiences.[9] While there is currently a lack of standardised language to describe immersive technologies, and a lack of consensus on the precise boundaries between these terms,[10] in this paper, we use the following terms:

- **Virtual reality (VR)** refers to immersive, completely digital, or simulated experiences typically reliant on head-mounted displays.[11] VR technologies can be used to create or access virtual worlds, which are persistent, 3D, real-time, immersive environments which

blur the line between physical and virtual, for socialising, working, learning, making transactions, playing and creating.[12] Social VR refers to multi-user VR environments.[13]

- **Mixed reality (MR)** enables both the overlay of digital elements into a view of the physical environment, and interaction between physical and digital elements.[14]
- **Augmented reality (AR)** inserts digital elements into a user's view of the physical environment [15] through devices like smartphones or AR glasses, and may include real-time sound and vision.
- **Extended reality (XR)** is an umbrella term that encompasses VR, MR and AR.[16]
- **The metaverse** refers to 'virtual worlds' that mirror the physical world, or blur the lines between the physical and digital world,[17] and which arguably have not yet fully materialised.[18] However, this term is continually evolving and definitions may vary. This paper does not focus specifically on the implications of the metaverse. This is because the development of the metaverse is at a much earlier stage compared to other forms of immersive technologies, and its future expansion is less certain. However, the risks and harms that may arise in the metaverse are likely to align closely with those identified in this paper. This position reflects consultation feedback from academic experts during the development of this paper.
- Haptic sensory technologies, or **haptics**, enable systems to simulate physical sensations like touch.[19] When combined with XR, haptics provide sensory feedback and allow users to 'feel' what is happening in the virtual environment.

Figure 1: Spectrum of immersive technologies[20]



How do immersive technologies work?

Immersive technologies aim to blend digital and physical elements in a seamless, interactive experience. This is achieved through human-computer interaction, made possible by the integration of software, hardware and sensors.

While different kinds of immersive technologies use different technical configurations, providing immersive experiences to users requires:

- a **Hardware interface** such as headsets, tablets, or handheld controllers, which include:
  - input devices (sensors) to collect data from a user (e.g. biometric data such as eye movements, facial expressions, location data, heartbeat, body movements) and/or the physical environment, and
  - output devices to deliver content to users (e.g. visual displays, haptics, speakers/headphones).
- **Software**, including real-time processing algorithms to process data collected and generate immersive content. This also includes operating systems, platforms, applications and 3D rendering engines.[21,22]
- **Computing power**, typically provided by smartphones, headsets or computing infrastructure.
- **Internet connectivity,** which is essential for most immersive platforms, such as immersive games and apps.

Social VR connects users across compatible devices, allowing them to participate in shared virtual environments in real time.

Using emerging technologies

Developers of immersive technologies aim to create an immersive experience for users.[23] In social VR environments, interfaces typically include voice and gaze interaction, motion controls, and body-tracking – features that enhance the user's sense of presence.[24] The embodied nature of VR, the synchronicity of interactions, and the perception of shared physical space can all serve to intensify the psychological impact of these experiences.[25]

Immersive technology products and services

In recent years, a wide range of XR devices and services have been developed and publicly released. Examples of some of these are shown in Figure 2.

Figure 2: Products in XR supply chain (selected)

Headsets & devices
Headsets: Meta Quest Pro, Apple Vision Pro, Sony PlayStation VR 2, Google, Microsoft HoloLens 2, Varjo XR-4, HTC Vive XR, ByteDance Pico 4, HTC Vive Pro Glasses: Meta Ray-Ban AI[26], Android XR[27]
OS
Meta OS, Apple Vision OS, Google Android XR, Open XR
Marketplaces
Meta Horizon Store, Steam Store, Viveport
Apps/content

Apps and content by Meta, Apple, Microsoft, Sony, Roblox
Social VR: Meta Horizon Worlds, RecRoom, VRChat

Immersive technology platforms may re-create a third-party developer ecosystem similar to the mobile environment, with third-party software development kits, plug-ins, and data sharing mechanisms built into the system.[28] Arguably, this has already occurred with marketplaces such as Meta's Horizon Store. Some XR products and services are being integrated with other new and emerging technologies, such as different types of AI. AI can enhance immersive experiences by improving processing power, enabling more detailed graphics, and creating more dynamic, responsive artificial elements.[29] AI can also be used to improve the ability of XR technologies to recognise objects and generate virtual representations of people.[30]

In addition, generative AI can be integrated into technologies that support immersive devices. For example, smart glasses could include integrated search functions powered by generative AI.

3.2 What are some current and projected applications of the technology? What benefits could the technology bring?

Immersive technologies have the potential to transform our relationships with digital information. They offer new ways to create immersive, interactive experiences that can improve outcomes across a wide range of domains.[31]

Current use cases are expanding across various industries and sectors, including:

- **Gaming:** Immersive technologies are widely used in gaming, where users can access 'immersive environments', through technologies such as VR.[32] For example, a wide range of games can be played with PlayStation VR or Meta Quest. An emerging industry of VR gaming centres also provide group-based experiences for parties and corporate events.[33]
- **Entertainment:** Immersive technologies can also be used to enhance entertainment experiences. For example, Apple markets its Vision Pro headset as a way to transform any room into a personal cinema.[34]
- **Retail:** Some brands are using immersive technologies to let shoppers browse virtual stores,[35] and to virtually try on their products.[36]
- **Engineering and architecture:** Immersive tools allow engineers and industrial designers to visualise, edit and share computer-aided design data as 3D holograms in real-world contexts.[37]
- **Training and education**: Immersive learning methods may offer greater educational benefits than traditional formats, particularly in disciplines that are abstract, conceptually complex, or focused on procedural learning.[38]

Other emerging applications span sectors such as healthcare (e.g. surgical simulations), art and education, as well as workplace induction and training across sectors.

Immersive technologies have the potential to enhance access to content and media, particularly for people with accessibility needs. For example, Apple's Vision Pro allows users to scroll with their eyes.

Additionally, while not a focus of this paper, possibilities for the convergence of immersive technologies and neurotechnology are growing. Neurotechnology is a rapidly expanding field of technologies dedicated to understanding and interacting with the brain or nervous system activity. XR devices already use sensors to track real-time user behaviour and future innovation

may see this sensor-based technology integrated with neurotechnological devices such as brain-computer interfaces (BCIs).[39]

There has also been significant public commentary about the potential emergence of 'virtual worlds' or metaverses relying on immersive technologies. Advances in enabling technologies, such as AI, the Internet of Things (IoT) and 5G/6G mobile networks, are improving the feasibility of 'next generation' virtual worlds.[40] In 2021, Meta described its vision of the metaverse to be the successor to the mobile internet.[41] However, significant doubt has since been cast about the potential of virtual worlds to provide all encompassing experiences.[42] In a memo to staff in early 2025, Meta's chief technology officer reportedly stated that "[t]his year likely determines whether this entire effort will go down as the work of visionaries or a legendary misadventure."[43]

3.3 What are some overarching limitations of the technology and drivers of risk?

Market projections for XR technologies vary significantly. For example, in 2024, Global Insights Services projected the 'XR market' would reach a market size of USD 450 billion by 2034,[44] while in 2025, Precedence Research projected a market size of USD 3,261.3 billion by 2034.[45]

Such discrepancies may reflect differing definitions for XR technologies. Further, some past predictions about the size of the XR market have proven to be overly optimistic,[46] and it is uncertain how immersive technologies will develop and how successful they will be.[47]

Immersive technologies currently face several technical limitations. Motion sickness in XR – which may be caused by factors such as high latency, low refresh rate, inaccurate hand tracking or low resolution[48] – may affect the user experience. Research indicates that the severity of symptoms associated with VR headset use increases with the duration of use, and may last for up to 4 hours after removal of the headset.[49] The quality of user experiences more broadly may also be impacted by current limitations to the quality of visual and auditory immersion, graphics quality, spatial audio accuracy, and haptic feedback. Inadequate internet speeds or WiFi connectivity may also contribute to these quality issues.[50,51]

The extent of interoperability across XR technologies supplied by different providers will influence how these technologies develop. Interoperability refers to the ability of different products and services from different digital platforms or other providers to work together and communicate with one another. Interoperability is forecast to be fundamental to the operation of the metaverse, and could enable a single, extended 3D environment rather than separate virtual worlds. Interoperability across major platforms could also accelerate the growth of the metaverse economy.[52] However, as discussed in section 4.4, interoperability between the immersive environments of different providers is currently low, and some forms of interoperability may be technically challenging.

The high prices of some immersive technology devices may have limited adoption by some users, although prices vary across devices. For example, the base model of the Apple Vision Pro retailed for AUD 5,999 in early 2025.[53] In comparison, the first Apple iPhone model released in Australia in 2008 cost AUD 735, or AUD 1,129 adjusted for inflation (2025).[54]

Immersive technologies may expose individuals to greater risks than other platforms and services, such as mobile phones or traditional social media. These could include:

- Heightened and different psychological and emotional responses. Research indicates immersive technologies can, in some circumstances, have a greater effect on the emotional response of users compared to less immersive forms of media.[55]

- More realistic social interactions, which can leave users more vulnerable to negative immersive experiences.
- The collection and use of larger amounts of user data, including biometric data.
- Challenges in protecting users' physical safety and online security.

Academic experts consulted in the development of this paper also highlighted that immersive technologies can reinforce existing barriers to inclusion. For example, VR systems often fail to account for the diverse ways in which people with disabilities move their bodies, limiting their effectiveness and usability.[56]

Risks to competition in the supply of immersive technologies include market concentration along the supply chain, and the potential for limitations in the interoperability of devices and services supplied by different firms.

As discussed in section 4, current and potential risks relating to immersive technologies intersect with the responsibilities of multiple regulators in Australia.

Where immersive technologies are integrated with generative AI models, many of the risks and limitations identified in DP-REG's working paper on multimodal foundation models may also apply.[57]

Other longer-term and more speculative risks will depend on how the technology evolves. For example, if technological innovations lead to hyper-realistic virtual environments, risks associated with certain types of content, conduct and interactions are likely to increase. While increased interoperability of different immersive technologies may benefit competition in the supply of immersive technologies, improved interoperability between platforms may allow harms in one environment to carry over into others.

4. Potential impacts and applicable regulatory frameworks

4.1 Overview

This section considers the potential impacts of immersive technologies across the regulatory remits of DP-REG members. Several cross-cutting themes highlight the importance of collaboration and coordination in addressing the various regulatory issues these technologies present.

Immersive technologies extend several of the multifaceted risks and harms apparent in other digital services. For example, data practices associated with XR products and services may have implications for privacy, as well as for groups that are particularly susceptible to harm, such as children and those experiencing gambling harm, or to types of harm, such as gender-based violence, and for competition between suppliers of these technologies. The convergence of immersive technologies and generative AI may also pose risks across different areas of regulation.

Immersive technologies may also pose enforcement challenges for regulators. For example, immersive environments may pose difficulties for users to capture evidence of harm and for regulators to detect harm, due to the fleeting nature of immersive interactions and the absence of URLs to pinpoint locations of harm.[58]

Other intersecting issues, such as the potential for immersive environments to facilitate criminal activity that may extend into the physical world, are outside the scope of this paper.[59] This working paper remains focused on impacts that align with the specific regulatory responsibilities of each DP-REG member.

4.2 Privacy

The Office of the Australian Information Commissioner (OAIC) is an independent Commonwealth regulator within the Attorney-General's portfolio. It brings together three functions: privacy, freedom of information, and information management. Its purpose is to promote and uphold Australians' privacy and information access rights.

Immersive technologies raise significant privacy risks due to their integration with the data of individual users. As these technologies evolve and their adoption grows, the scale and nature of these risks are expected to increase.

Risk of extensive data collection, use and disclosure

Immersive technologies have the potential to collect and store a wide range of information about a user. This includes:

- **Personal information:** Includes a broad range of information, or an opinion, that could identify an individual – such as name, address, date of birth, location, or sensitive information.
- **Sensitive information:** A subset of personal information, including details about an individual's racial or ethnic origin, religious beliefs, political opinions, or health information.
- **Sensor information (biometric and physiological information):** Data based on physiological or behavioural characteristics that can be used to identify a person. Physiological biometrics could include fingerprints, face, or hand geometry. Behavioural biometrics may include a person's signature patterns or keystroke dynamics.
- **Psychographic data:** Information about user preferences, interests and values, inferred from behaviours, actions, and reactions during immersive experiences.[60]
- **Spatial data:** Information about the movement, location, and dimensions of people or objects in a virtual environment. XR devices capture and process data such as gestures and eye tracking to create immersive experiences.

The collection, use and disclosure of personal and sensitive information must comply with the Australian Privacy Principles (APPs) to ensure entities are complying with their privacy and security obligations. Entities are expected to comply with their privacy and security obligations and obtain informed and meaningful consent at all times.

Immersive technologies may also collect data about bystanders – for example, by capturing information from a user's physical environment in public spaces. Because bystanders cannot provide informed consent to this data being collected, used or disclosed, it is the responsibility of entities to ensure the privacy rights of these individuals are respected.

There are also specific risks related to children. As immersive technologies are increasingly used for gaming, social interaction and education, there is a heightened risk of collecting large volumes of personal and sensitive information from children. In the United States, the Federal Trade Commission (FTC) has been asked to investigate allegations that Meta knowingly allowed children under 13 to access its Horizon Worlds gaming platform through their VR headsets and collected their data without parental notice or consent.

In Australia, this vulnerability is being addressed through new privacy laws. Following the passage of the *Privacy and Other Legislation Amendment Act 2024* (Cth)[61] the OAIC is developing a Children's Online Privacy Code. The Code will enhance privacy protections for

children who engage in the digital world, where large amounts of personal information are collected from an early age. The aim is not to prevent children from participating online, but to ensure they are protected – particularly in how their personal data is handled.

While the primary objective of the Code is to improve privacy protections for children, this initiative also aims to set broader standards that lift privacy practices for all Australians. The Code aims to embed stronger privacy protections into digital systems and promote a more transparent and accountable online environment for all users.

Risks associated with data sharing

Third parties

A critical privacy risk for users is the limited transparency around how their personal and sensitive information is used and shared. The development and operation of immersive technology platforms typically involve multiple parties, such as app developers, hardware manufacturers, and analytics providers. These parties may collect or share data for purposes beyond the original intent.

Data sharing with third parties increases the risk of breaches, particularly where robust data protection controls are not in place. A lack of transparency about what data is collected, how long it is stored, and who has access to it may result in user profiling, targeted advertising, and behavioural manipulation through personalised content.

Privacy issues related to interoperability

Interoperability could enable a seamless digital identity experience across multiple platforms, but may also raise significant privacy and data management concerns. If widely adopted in immersive technologies, interoperability may eliminate the need for users to log in separately across services, bypassing repeated acceptance of terms and conditions, for example if accompanied by single sign-on authentication methods. However, uncertainty about how personal and sensitive information flows between different 'environments' could lead to privacy issues – particularly where data crosses multiple jurisdictions.

Profiling and targeted advertising

The collection of data and subsequent sharing with third parties can lead to the profiling of individuals and targeted advertising based on personal and sensitive information.

According to research by Dr Joanne Gray from the University of Sydney, immersive technologies function on the collection of data and can collect up to 90 pieces of data per second from a single user. This extensive psychographic data collection allows entities to infer highly sensitive information – such as a user's emotional state, mental wellbeing, and decision-making patterns – raising the risk of manipulation through targeted and personalised advertising.[62]

The inability to provide meaningful consent to the collection of such psychographic data – particularly bodily responses to immersive stimuli – poses a serious privacy risk. When used to record preferences and serve tailored advertising, this data can shape user experience in ways the individual may not fully understand or control.

Privacy by design

‘Privacy by design’ refers to the practice of embedding strong privacy practices into the design of technologies, business processes, and physical infrastructure from the outset. Rather than retrofitting safeguards after privacy issues arise, this approach proactively manages risk – building trust and ensuring compliance. Privacy by design is particularly important in the context of immersive technologies, which often rely on extensive collection of personal and sensitive information.

The privacy risks identified above can be managed through the consistent application of good privacy practices. Given the global nature of many entities operating in this space, this will require significant cooperation between businesses and privacy regulators across jurisdictions.

Currently, some immersive platforms do not allow users to opt out of certain high-risk features, such as environmental data capture or eye tracking, as these are built into device functionality.[63] Device operation should not be dependent on the collection of personal or sensitive information. Privacy protections should be integrated from the outset and include measures such as:

- designing immersive technologies with privacy in mind from the beginning
- conducting a privacy impact assessment as an iterative process throughout the development of the product and the product lifecycle
- ensuring proactive compliance with the APPs
- embedding user consent controls into platforms
- making privacy the default – for example, keeping features such as location sharing or eye tracking off until the user turns them on
- applying data minimisation, retention and destruction policies
- ensuring data is user centric – allowing individuals to easily access, correct and delete their data.

As immersive technologies become more widely accessible, strong privacy protections must remain a priority throughout the entire lifecycle of these products. Without appropriate regulation of the collection, use, and disclosure of highly sensitive data, users may face a growing range of risks.

4.3 Consumer protection

The Australian Competition and Consumer Commission’s (ACCC) role includes enforcing the Australian Consumer Law (ACL), which prohibits misleading and deceptive conduct, unconscionable conduct, and unfair contract terms used in standard form contracts with consumers or small businesses. The ACL also regulates unsafe products, promotes fair trading, and provides for automatic consumer guarantee rights (enforceable by consumers) in the supply of products and services. The ACL applies to all consumer products or services other than financial products and services.[64]

There are also a range of unfair trading practices that may cause consumer harm, including conduct that distorts, manipulates or undermines consumer choice, which currently fall outside of the ACL.[65] Some of these harms have the potential to arise in immersive technology markets.

The ACCC also operates the National Anti-Scam Centre (NASC) and the Scamwatch website, which helps Australians to recognise, report, and protect themselves from scams.

Product safety issues

Immersive devices present new risks to the safety of consumers that may result in harm. This includes harms that may arise in devices that are functioning as intended. Users of immersive devices may experience cybersickness, visual fatigue, muscular fatigue, and acute stress.[66] Other risks related to the use of immersive devices may include fire or heat hazards, electrical hazards, and injury due to headset wiring.[67]

These devices may also be a source of risks to the safety of consumers because of their potential to cause distraction and disorientation,[68] which may contribute to injury due to loss of balance (e.g. falls), or the user not being aware of the surrounding environment (e.g. collision with objects).[69]

Other consumer protection issues

The ACL contains prohibitions on misleading or deceptive conduct, and false or misleading representations.

As firms seek to sell a vision of a fully realised metaverse or virtual world which is not yet available, there is a risk that advertising of immersive devices may mislead consumers about the functionality of immersive devices and spaces. Further, the integration of XR technologies with generative AI could increase the potential for misleading or deceptive conduct in immersive environments.[70] For example, deepfakes that take the form of a 3D person could be used to mislead consumers about celebrity endorsements, or otherwise influence their purchasing decisions more effectively than traditional formats, such as video. The realism and emotional intensity of immersive environments may amplify these effects.

By tracking and interpreting a range of user data, XR headsets may also facilitate enhanced manipulation of consumers, such as through behavioural nudging or the use of deceptive design.[71] A 2024 literature review found that while most deceptive design in XR demonstrated similar attributes to those on the web, the deceptive design in XR used more subtle influence mechanisms and more accurate targeting of individual users' weaknesses, resulting in manipulations that are novel, unfamiliar and challenging to detect.[72]

The ACCC's Final Report of the Digital Platform Services Inquiry, which considered potential consumer harms in online gaming, noted that while immersion has long been recognised as an important aspect of successful game design, online game players, particularly those heavily immersed or invested in a game, may be susceptible to interface design practices present in some online games which exploit cognitive biases or manipulate them into making in-game purchases.[73]

Many XR applications currently rely on mobile operating systems and smartphones, allowing traditional manipulative design practices (dark patterns) used in mobile apps to be applied to immersive apps. These include, for example, cumbersome menus to disable default settings or misleading information in 2D menu interfaces.[74]

There are also likely to be complex supply chains in the immersive technology sector, where multiple suppliers are involved in offering and supplying products and services to consumers. This contrasts with traditional supply chains, where there is a clear movement of products (from manufacturer, to retailer, to consumer). Any parties in the supply chain can impact the goods and services that consumers acquire, and attribution of liability for issues that arise is not straightforward. This complexity has implications for many aspects of the consumer law, including consumer guarantees and manufacturer liability for products with a safety defect.

Scams

Immersive technologies may introduce new channels for potential scams.[75] While currently a largely theoretical risk, existing types of internet scams may move into the metaverse,

potentially causing heightened psychological harm because of the immersive nature of the user experience.[76]

For example, 'inception attacks' have been shown to be viable and effective. Named after the 2010 Christopher Nolan film, inception attacks involve an attacker controlling and manipulating a user's interaction with their VR system, by trapping them inside a single, malicious VR app that masquerades as the full VR system.[77] In a 2024 study, researchers successfully simulated 3 attacks using the Meta Quest Browser app, the built-in web browser for Quest headsets. These attacks included modifying the display of a target's bank balance and manipulating the payment amount input by the user.[78]

Scams in immersive environments may also be facilitated by advertising, similar to the ways in which advertising can facilitate scams in less immersive contexts, such as social media.[79] The highly intimate, personalised data that is collected through immersive technologies can be leveraged to tailor advertising in immersive environments to each user.[80] Advertising in immersive contexts, specifically AR, has been shown to increase customers' willingness to pay relative to traditional 2D advertising, and immersive environments may also interfere with a user's sense of the 'reality' of financial consequences.[81]

4.4 Competition

The ACCC has a key role promoting competition by administering and enforcing the *Competition and Consumer Act 2010* (Cth) and other legislation. This includes enforcing prohibitions of cartel conduct, misuse of market power, anti-competitive exclusive dealing, resale price maintenance and certain conduct that has the purpose, effect, or likely effect of substantially lessening competition in a market. The ACCC also administers the merger control regime, and has regulatory functions in some national infrastructure industries (such as access to telecommunications services), and undertakes price inquiries as directed by the Treasurer (such as the Digital Platform Services Inquiry 2020-2025, which concluded in March 2025).

Effective competition drives firms to innovate, and to improve the quality and price of the products and services they offer to consumers. In the context of immersive technologies, competition may occur at different levels of the supply chain – from the design and manufacture of devices (e.g. headsets, glasses) and device components (e.g. cameras, motion sensors, visual display parts) to the supply of software, apps, and platforms that enable immersive experiences.

Potential barriers to entry and expansion

The supply of immersive technologies may be impacted by several barriers to entry and expansion.

- **Barriers to interoperability**: While interoperability can potentially raise privacy and safety issues, as discussed in sections 4.2 and 4.6, interoperability can benefit competition in terms of encouraging innovation and reducing friction for consumers. In 2023, the United Kingdom's (UK) Digital Regulation Cooperation Forum (DRCF) – which brings together four UK regulators with responsibilities for digital regulation (the Competition and Markets Authority (CMA), Financial Conduct Authority (FCA), the Information Commissioner's Office (ICO) and the Office of Communications (Ofcom) - noted there was low interoperability between immersive environments from different providers, in terms of the ability of a user to seamlessly transfer information such as settings, preferences, and other data between environments, and further noted uncertainty regarding whether interoperability would remain at a low level or develop further.[82] Also in 2023, the UK CMA noted that factors such as the existence of technical

barriers to standardisation, and varying incentives to support it, seem to have limited immersive environments from deeper interoperability for now.[83]

Vertical interoperability may unlock access to markets downstream of platforms or services, especially in ecosystems that remain 'closed' or heavily vertically integrated. This could allow new entrants to compete on more equal terms with vertically integrated products.[84] For example, greater interoperability between proprietary immersive worlds and a variety of XR headsets could increase competition in headset supply. Similarly, allowing a proprietary headset to support a broader range of third-party apps could promote competition for the supply of such apps.

There have also been widespread calls for horizontal interoperability in immersive environments, and for the portability of data generated by avatars, users, and devices, and digital assets, across different services without friction.[85] However, in some cases, increased interoperability may be technically challenging and result in unintended trade-offs, including in terms of security and innovation, in addition to the privacy and online safety concerns addressed in this paper.[86]

- **Network effects:** Social VR platforms and virtual worlds with large user bases may benefit from network effects that provide competitive advantages that rival firms may find difficult to overcome. This is because their value to consumers increases based on the number of other users on the service (same-side network effects) and their value to advertisers increases based on the number of end users (cross-side network effects). Network effects involving access to high-quality data may also apply, where immersive technology device and platform usage generates data that helps improve the product or service.[87]
- **Economies of scale and scope:** XR hardware and software is often costly and complex to develop and maintain.[88] For example, Meta's Reality Labs has reported operating losses of more than USD 60 billion (approximately AUD 94 billion) since 2020, with its largest loss reported in the fourth quarter of 2024.[89] To the extent that investments in developing the necessary hardware and software are a sunk cost, this implies a potentially significant barrier to entry. In addition, adding data collected through immersive technologies to the offerings of firms that have already accumulated large pools of proprietary user data through other services in which they are dominant, may amplify economies of scope.[90]
- **Compute capabilities:** Supplying immersive experiences requires substantial computing resources to process large volumes of data at high speed. Cloud computing is increasingly used to stream otherwise graphically demanding experiences from less computationally capable devices, such as headsets.[91] Because the supply of enterprise cloud computing services is concentrated,[92] firms that have access to these resources through their presence in the cloud supply chain, such as Amazon, Microsoft and Google, may have an advantage in the supply of compute intensive immersive technologies.

As immersive technologies become more common, monitoring by competition authorities will be important to assess whether the potential for new entry and expansion is sufficient to constrain incumbent firms.

Concluding comment on competition and consumer issues

Relevant to the ACCC's consideration of the implications of immersive technologies for competition and consumers, the ACCC's compliance and enforcement priorities for 2025-26 include a focus on competition, product safety, consumer and fair trading issues in the digital

economy, and on improving industry compliance with consumer guarantees with a focus on consumer electronics.[93]

4.5 Media and the information environment

The Australian Communications and Media Authority (ACMA) is Australia's independent regulator for media and communications. The ACMA regulates broadcasting and some aspects of online content delivered by digital platform services in Australia. It also oversees the voluntary Australian Code of Practice on Disinformation and Misinformation and has powers to combat phone and SMS scams.

The adoption of immersive technologies is still in its early stages across the economy. Entertainment and online gaming have been early markets for these technologies, leveraging existing audiences. However, as take-up expands, potential risks have been identified – many of which may exacerbate existing harms that fall within the ACMA's remit.

Online gambling

The sophistication of immersive technologies – particularly virtual reality – is likely to exacerbate the addictive aspects of online gambling for some players.[94] The heightened sensory engagement offered by immersive experiences may intensify psychological rewards, which can lead to potentially problematic use.[95] The integration of virtual reality with existing personalisation and analytics tools, which tailor gambling experiences to individual users, may further exacerbate these risks.

Conversely, the same features that heighten gambling-related harms could also be used to promote responsible gambling practices. For example, immersive technologies can collect a broad range of sensory data, including emotional responses to stimuli. These markers could be used to trigger alerts encouraging players to take breaks when signs of stress are detected.

Immersive technologies may also open up additional markets for online gambling, including for some services that are illegal in Australia. These illegal services do not offer the same protections as Australian licensed services.

Gambling advertising

Immersive technologies may create more opportunities for gambling services to advertise to Australians. For example, virtual reality scenarios could recreate actual sporting matches with gambling advertisements displayed alongside real-time statistics, odds and scores. This could encourage vulnerable users to make bets, particularly given the ease and immediacy with which they could do so.[96] This type of integrated advertising could become an appealing part of the viewing experience – not only in sporting contexts but also during gaming, esports or other forms of immersive entertainment.

Information integrity

Traditionally, audiences – whether online or via broadcast television and radio – have relied on signals to determine the authenticity and integrity of information. Immersive technologies could create introduce additional challenges to determining the provenance of content, compounding the risks already posed by the rise of AI-generated material. This heightens the potential for deepfakes, disinformation and misinformation.

As immersive technologies continue to evolve, they are capable of creating highly realistic environments. For example, the Christchurch shooting massacre was re-created on the Roblox platform. As users gain the ability to build more lifelike virtual worlds, the risk of misinformation and disinformation about historical events may increase.

Another risk to information integrity involves the difficulty of moderating behaviour and conduct in immersive spaces. Because these technologies accumulate highly individualised body-based data, users may be more susceptible to targeted disinformation and misinformation campaigns. The integration of generative AI further compounds this risk by enabling influence campaigns that can be scaled and tailored to each user.[97]

Accessibility

Immersive technologies have the potential to enhance access to content and media, particularly for people with accessibility needs. For example, Apple's Vision Pro allows users to scroll with their eyes.

However, many of these services require high bandwidth and specialised equipment for access. This may lead to unequal access – especially for those who stand to benefit most from these technologies.

Without appropriate safeguards or transparency, the data collected through immersive technologies may also be misused – for example, in scams, spam, or targeted advertising. This poses additional risks for vulnerable users.

4.6 Online safety

eSafety is Australia's independent regulator and educator for online safety. The *Online Safety Act 2021* (Cth) (OSA) gives eSafety a range of regulatory powers to protect Australians from harm and promote safer online experiences. These powers include complaints schemes, industry codes and standards, the Basic Online Safety Expectations, and implementation of the social media minimum age obligations under Part 4A of the OSA.

eSafety has long recognised that the online world offers a mix of benefits and harms. Immersive technologies enable 3D interactions and real-time experiences that transcend geographical barriers and the limitations of traditional 2D media. While these features can offer benefits, they may also lead to new ways to perpetrate abuse.

In May 2025, eSafety released an updated position paper on immersive technologies. The paper outlines the online safety risks, harms, benefits and opportunities of immersive technologies. It also explores regulatory challenges, including how immersive technologies fit within eSafety's regulatory remit, and proposes Safety by Design measures industry can adopt to mitigate safety risks.

Interoperability

Interoperability has implications for online safety. A potential benefit is the ability for safety settings to carry over between platforms or environments. However, without proper safeguards, interoperability could increase online safety risks. For example, it could allow children to move between platforms without restriction or detection, increasing their risk of exposure to age-inappropriate content and experiences. Safety must be embedded in the design and implementation of interoperable systems.

Interoperability may also have implications for data management. A user may consent to sharing personal information with one platform but not another.[98] As it is possible that immersive technologies may evolve toward greater interoperability, privacy and security must be considered alongside safety.

Convergence of technologies

Immersive technologies are increasingly integrated with other technologies such as AI and algorithms to enhance personalisation. For example, generative AI can create visual elements within immersive environments, including non-player characters. AI algorithms are also used to process user data to predict behaviour and interests, allowing for more tailored and responsive experiences. As AI can analyse and process large volumes of data and generate predictive outputs rapidly, these personalised responses can be generated almost instantly in immersive environments.

However, this convergence also increases safety risks. Generative AI algorithms may generate harmful content, which could have a more visceral and intense impact in immersive environments. While integrating technologies may improve their functionality and efficiency, safety must be embedded throughout the technology lifecycle to prevent harms from compounding.

Amplification of existing content, conduct, contact harms

Harms that people already experience offline and in 2D online environments may be amplified in immersive settings. The novel features offered by immersive technologies – such as their hyper-realistic, embodied, and cross-dimensional qualities – can intensify existing harms and give rise to new manifestations of them.

Several forms of online harm are likely to be heightened in immersive environments.

Terrorism and violent extremism

Perpetrators of terrorism and violent extremism could weaponise immersive technologies to enhance their coordination, propaganda, and indoctrination efforts.

The interactive nature of immersive environments may amplify the effect of echo chambers,[99] enabling terrorist and violent extremist groups to perpetuate their ideologies and increasing the risk of recruitment and radicalisation.

There have been instances of users recreating and role-playing terror attacks on immersive platforms popular with children and young people, raising serious concerns about exposure to extremist ideologies and the potential for radicalisation.[100]

Additionally, wearable XR devices, such as AR smart glasses, could be used to livestream terror attacks.[101]

Child sexual exploitation and abuse (CSEA)

Abusers may exploit immersive technologies to create new avenues for illegal and inappropriate contact, conduct, and engagement with children.

Abusers can weaponise the anonymity afforded by avatars to approach and groom children, who may believe they are interacting with a peer rather than an adult. In immersive environments, this anonymity combines with expressive features such as gestures, movement, and body language – potentially increasing an abuser's ability to build trust and rapport.[102]

Abusers may engage in sexualised conversations, perpetrate sexually exploitative or abusive activities towards children, or coerce children into performing sexual movements on immersive platforms.[103] Once abusers establish contact and trust, they may move their interactions to other platforms – such as encrypted 2D messaging platforms – where detection is less likely. In these settings, abusers may coerce children to produce CSEA material of themselves or coerce children into offline interactions.[104]

There are also growing concerns about how immersive technologies may be used to access CSEA material. For example, there have already been cases of abusers using VR headsets to view and store CSEA material.[105]

Exposure to age-inappropriate content and experiences for children

Immersive technologies may amplify the risk and impact of children encountering age-inappropriate content, such as pornography or violent material. When interacting in a 3D, immersive environment, such material can be more visceral than when viewed on a 2D screen.

Further studies into the impact of immersive technologies on children and young people are required. However, existing research indicates that children may experience VR in ways similar to how they experience physical reality.[106] The illusion of VR may be more effective on young children and those who are still developing the critical reasoning skills needed to distinguish between events which happen in the virtual world and events in the physical world.[107]

Sextortion and image-based abuse

Immersive technologies present enhanced risks for sexual harms which already occur on traditional 2D platforms, such as sexual extortion.[108] For example, a user may engage in what they believe is a private interaction within an immersive space, only for the interaction to be recorded without their consent and threatened to be shared unless the user complies with the demands of the other party.

Avatar-based interactions have also introduced new ways to perpetrate sexual harms. eSafety's metaverse research found that 6% of metaverse users who were surveyed (n=259) reported someone had created a sexually explicit avatar of them to interact with, without their consent.[109]

When combined with generative AI, immersive technologies can be used to create and share lifelike intimate scenarios involving people without their knowledge or permission.

Tech-facilitated gender-based violence (TFGBV)

Gender-based violence (GBV) is any form of physical or non-physical violence or abuse against a person or group because of biased or harmful beliefs about gender.

TFGBV is where GBV is facilitated by technologies. It includes technology-facilitated behaviours such as sexual harassment, misogynistic comments, homophobic language, stalking, coercive control, image-based abuse, and threats of sexual violence. These behaviours are already prevalent online[110] and are now occurring in immersive spaces.

The hyperrealism and real-time nature of immersive technologies allow perpetrators to go beyond the limitations of 2D platforms and 'act out' threats of sexual violence and harassment. In a survey of more than 600 users of popular VR devices, 49% of women respondents reported experiencing sexual harassment in VR environments. Reported behaviours included groping, stalking, catcalling, being shown explicit images, and receiving sexually explicit comments.[111]

The misuse of immersive technologies has also led to the rise of 'embodied harassment',[112] a term that describes unwanted behaviours facilitated by avatars in immersive spaces. It can include actions such as unwanted touching or groping of another person's avatar, performing unwanted sexual gestures towards another person's avatar, or invading another avatar's personal space.

Negative online social experiences

Negative online social experiences that occur on 2D platforms also persist in immersive environments. The hyper-realistic nature of immersive technologies can intensify the impact of these interactions.

In immersive environments, harassing behaviours such as stalking and unwanted contact may feel more invasive than harassment on traditional social media. Where perpetrators were once confined to a 2D screen, immersive technologies can make it appear as though they are physically following other users or invading their personal space. This means the onus is often wrongly on users to safely remove themselves from abusive situations and makes it more difficult for them to do so. The real-time and often ephemeral nature of these interactions may also create barriers to reporting harmful behaviour or seeking remedial action.

eSafety's approach to online safety

eSafety's approach to online safety is built on three pillars: prevention, protection, and proactive, systemic change.

Prevention

Understanding the benefits and risks of immersive technologies can help people to better manage their online experiences and contribute to a safer, more positive online environment. eSafety supports this through age-appropriate education programs and resources that promote digital literacy, critical thinking, and online resilience.

eSafety also provides practical tools and guidance. The online tools and features page on immersive technologies offers advice about their safe use, while eSafety's Gift Guide helps people make safety-conscious choices when buying popular tech gifts, including immersive products.

Protection

eSafety offers tangible, rapid support to Australians who experience online harm. Through its complaints schemes, eSafety can respond to reports of adult cyber abuse, child cyberbullying, image-based abuse, and illegal or restricted content that is class 1 and class 2 material.

eSafety provides support to people who make complaints under these complaints schemes by offering guidance, assisting in or requiring the removal of certain content, and minimising the risk of further harm.

It is possible that experiences facilitated by immersive technologies may add complexity for the collection of evidence in investigations. Under the Online Safety Act (OSA), eSafety's existing suite of remedies for complaints focuses primarily on the removal of material. This may present limitations on how eSafety can respond to complaints of harm in immersive environments – which allow for synchronous, ephemeral virtual experiences and may have limitations for capturing content in real time or retrospectively – where that harm has not been captured in material form.

Proactive and systemic change

To stay abreast of emerging online harms, eSafety uses its systemic regulatory powers under the OSA. These include enforceable industry codes and standards and the Basic Online Safety Expectations.

The Industry Codes and Standards are designed to protect Australians from illegal and restricted online content, by setting mandatory and enforceable obligations for eight sections of the online industry to proactively address this material at a systemic level.[113] This approach seeks to enforce safety obligations across every aspect of the technology stack.

The various layers that comprise an immersive experience will have different requirements under the codes and standards. For example:

- Providers that manufacture XR headsets may be subject to requirements set out in the Equipment Online Safety Code (Class 1A and Class 1B Material) (Equipment Code), such as providing annual compliance reports and enabling users to report potential Code breaches.
- If another provider or the same provider operates a service that enables end-users to download apps to use in immersive environments, then that service is likely to be subject to the App Distribution Services Online Safety Code (Class 1A and Class 1B Material).
- Providers offering XR services and apps may be subject to the Online Safety (Designated Internet Services— Class 1A and Class 1B Material) Industry Standard 2024. If they have a messaging or chat functionality, they are likely to be subject to the Online Safety (Relevant Electronic Services – Class 1A and 1B Material) Industry Standard 2024.[114]

The OSA also empowers eSafety to require social media services, relevant electronic services (such as messaging, gaming, and dating services), and designated internet services (such as other apps and websites) to report on the reasonable steps they are taking to comply with the Australian Government's Basic Online Safety Expectations (the Expectations). This is to make sure these services are transparent, accountable, and safe for people to use. eSafety has the power to compel information from online providers and publish information about the steps they are taking to meet the Expectations in transparency reports. Future reports could cover immersive platforms and functionalities.

A key initiative driving systemic change is eSafety's Safety by Design, which is built on three foundational principles: service provider responsibility, user empowerment and autonomy, and transparency and accountability.

Immersive technology companies can uphold these principles by incorporating safety measures throughout the entire lifecycle of their products – from design and development to deployment.

Additionally, as part of eSafety's work as an anticipatory regulator, eSafety conducts horizon scanning and engages with subject matter experts through its Tech Trends and Challenges program. This allows eSafety to identify the online safety risks and benefits of emerging technologies and to understand the regulatory opportunities and challenges they may present.

5. Australian Government developments

Below we highlight regulatory developments relevant to the remits of DP-REG members. Some of these developments may strengthen the capacity of regulators to address emerging risks associated with immersive technologies.

Online safety

Phase 2 Industry codes

Development of the Phase 2 industry codes formally commenced in July 2024 with the publication of eSafety's Phase 2 position paper and the issuing of notices to industry to develop the Phase 2 industry codes.

The Phase 2 codes cover 'class 1C' and 'class 2' material – defined under the National Classification Scheme – which includes online pornography, simulated gambling, and content featuring themes such as suicide.

The aims of the Phase 2 industry codes are to prevent children from accessing or being exposed to age-inappropriate material online (including material like online pornography) and to provide all end-users with effective information, tools and options to limit access and exposure to such material. It is likely the various layers that comprise an immersive experience will have different requirements under the Phase 2 industry codes.

The industry associations submitted seven industry codes to eSafety for review on 28 February 2025, and the eighth code (for app distribution services) was submitted to eSafety on 28 March 2025.

In April 2025, the eSafety Commissioner advised industry of her preliminary view that the submitted codes would not provide the appropriate community safeguards required for them to be registered. Industry was provided with the opportunity to submit final revised codes for review by 20 May 2025. eSafety received the final draft codes.

In June 2025, the eSafety Commissioner registered three of the nine revised codes. These cover search engine services, enterprise hosting services, and internet carriage services, such as telcos. The Commissioner sought additional safety commitments from industry on the remaining codes.

In September 2025, the eSafety Commissioner registered the six remaining codes. These apply to a broad range of online services and platforms — including app stores, gaming services, pornography websites, generative AI services and AI companion chatbots, equipment manufacturers and suppliers. They also apply to social media services, with one code covering 'core' features such as posting content on the service and another covering their messaging features.

Social Media Minimum Age Obligation

Part 4A of the OSA will require age-restricted social media platforms to take reasonable steps to prevent children under 16 from having an account.

On 29 July 2025, the Minister for Communications made legislative rules clarifying which types of services are excluded from the age restriction.

From 10 December 2025, age-restricted social media platforms will have to take reasonable steps to prevent Australians under the age of 16 from creating or keeping an account.

Review of the *Online Safety Act 2021* (Cth)

In 2024, Ms Delia Rickard PSM conducted an independent review of the OSA. The independent review examined the operation and effectiveness of the OSA and considered whether additional

protections are needed to combat online harms, including those posed by emerging technologies.

The Final Report of the review was provided to the Australian Government on 31 October 2024. This was tabled in parliament on 4 February 2025. A digital duty of care model is a key recommendation of the statutory review into the OSA. In November 2024, the Government announced its intention to legislate a Digital Duty of Care.

Privacy

The Office of the Australian Information Commissioner (OAIC) welcomed passage of the Privacy and Other Legislation Amendment Act 2024 as a significant step forward in strengthening privacy protections for Australians.

A key reform under the Act is the requirement for the OAIC to develop a Children's Online Privacy Code. This code will apply to social media platforms and other online services that are likely to be accessed by children. The OAIC is currently consulting on and developing the Code.

The OAIC has also published guidance on AI and privacy:

- Privacy and developing and training generative AI models
- Privacy and the use of commercially available AI products.

Consumer protection and competition

Proposed new digital competition regime

Between December 2024 and February 2025, the Treasury consulted on the Government's proposals for the legislative implementation of a new digital competition regime. The new digital competition regime would apply to certain large digital platforms with a critical position in the Australian economy and that are significant to Australian consumers and businesses, in respect of specific services they supply.

Review of AI and the Australian Consumer Law

In 2024, the Treasury consulted on whether the ACL remains suitable to protect consumers who use AI, and to support the safe and responsible use of AI by businesses. The purpose of this review was to inform other ongoing work, on Australia's consumer protection framework and work to clarify and strengthen existing laws to address AI-related risks and harms. In the context of immersive technologies, this work is particularly relevant to XR products and services that integrate AI.[115]

6. Overseas developments

General developments

In recent years, a range of regulators and policymakers around the world have focused on better understanding immersive technologies, and their implications for individuals, businesses and society.

In 2025, the Organisation for Economic Co-operation and Development (OECD) released an immersive technology primer identifying and analysing developments in immersive technologies, their potential socioeconomic impacts, and implications for policy.[116]

In the UK, the DRCF published an Immersive Technologies Foresight Paper in 2023. The paper explored the future of immersive technologies, including key uncertainties that could drive changes to them, as well as related benefits and risks.

In 2022, the European Commission (EC) launched the Virtual and Augmented Reality Industrial Coalition, a platform for structured dialogue between the European VR/AR ecosystem and policymakers. In 2023, the EC released its strategy on Web 4.0 and virtual worlds, intended to steer the next technological transition and ensure an open, secure, trustworthy, fair and inclusive digital environment for European Union (EU) citizens, businesses and public administrations. The EC also launched a related pilot project in 2024 to inform policy makers and stakeholders of the challenges and governance needs arising from the development of cutting-edge virtual world and web 4.0 technologies, and foster discussion on global governance.

Privacy

The UK's data protection regulator, the Information Commissioner's Office (ICO) released its Tech Horizons Report for 2024, focusing on a range of topics, including immersive virtual worlds.

Consumer protection and competition

In 2023, the CMA published Trends in Digital Markets: a CMA horizon scanning report, which considered 10 trends in digital markets the CMA believed would have an impact on digital markets in the following 5 years and beyond, which included trends related to immersive technologies.

In 2024, the EC called for submissions on competition in virtual worlds from interested stakeholders, and sent requests for information to several large digital firms, citing the importance of competition for growth and innovation in this new market.[117]

7. Conclusion

Immersive technologies have emerged as a new frontier for innovation, offering Australians and Australian businesses a wide range of potential benefits.

At the same time, policy and regulatory responses to these technologies must reflect that these benefits will not be fully realised unless their potential to create and exacerbate a range of harms is also understood and mitigated.

Many of the risks are already clear and often mirror or extend those identified by DP-REG members in the context of related digital platform services. As immersive technologies and their use cases continue to evolve, it will be important to minimise their potential to cause or facilitate harm.

These technologies also raise cross-cutting issues and shared challenges. As digital regulators, we recognise the intersections between the risks and harms that fall within our respective remits, and the value of coordinated action. DP-REG members will continue to apply our existing regulatory frameworks and work with government to ensure the digital economy is a safe, trusted, fair, innovative and competitive space.

8. Acknowledgements

In preparing this paper, DP-REG benefited from the insights on immersive technologies generously shared by the following experts:

- Dr. Joanne Gray, The University of Sydney
- Dr. Ben Egliston, The University of Sydney
- Dr. Benjamin Tag, The University of New South Wales
- Brittan Heller, Stanford University
- Prof. Marcus Carter, The University of Sydney

9. Endnotes

[1] Vítor Bernardo, European Data Protection Supervisor, European Commission, Extended Reality, accessed 11 September 2025
[2] Department of the Treasury, Digital platforms – a proposed new digital competition regime, 2 December 2024, accessed 11 September 2025
Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts, Statutory Review of the Online Safety Act 2021, 2025, accessed 11 September 2025
[3] Parliament of Australia, Privacy and Other Legislation Amendment Bill 2024, 2024, accessed 11 September 2025; Parliament of Australia, Scams Prevention Framework Bill 2025, 2025, accessed 11 September 2025
[4] Digital Platform Regulators Forum (DP-REG), Communique | Digital Platform Regulators Forum 2024, 25 July 2024, accessed 11 September 2025
[5] eSafety, Tech Trends position paper: Immersive technologies, May 2025, accessed 11 September 2025, p 5
[6] M Vasarainen et al, A Systematic Literature Review on Extended Reality: Virtual, Augmented and Mixed Reality in Working Life, October 2021, accessed 11 September 2025, p 4
[7] M Vasarainen et al, A Systematic Literature Review on Extended Reality: Virtual, Augmented and Mixed Reality in Working Life, October 2021, accessed 11 September 2025, p 4
[8] Digital Regulation Cooperation Forum (DRCF), Immersive Technologies Foresight Paper, December 2023, accessed 11 September 2021, p 1
[9] For example, see Commonwealth Scientific and Industrial Research Organisation (CSIRO), Virtual reality smells like spleen spirit, 4 April 2022, accessed 11 September 2025; BBC, Press to sniff: Can smelling a game make it more immersive?, 1 February 2025, accessed 11 September 2025; Digital Trends, VR wearable can simulate temperature changes using odorless chemicals, 30 June 2020, accessed 11 September 2025
[10] I Hupont Torres et al, European Commission, Next Generation Virtual Worlds: Societal, Technological, Economic and Policy Challenges for the EU, July 2023, accessed 11 September 2025, p 10
[11] J Gray, M Carter & B Egliston, Governing Social Virtual Reality: Preparing for the Content, Conduct and Design Challenges of Immersive Social Media , 2024, accessed 11 September 2025, p 4
[12] European Commission, Staff Working Document: information, insights and market trends on web 4.0 and virtual worlds, 11 July 2023, p 87.
[13] J Gray M Carter & B Egliston, Governing Social Virtual Reality: Preparing for the Content, Conduct and Design Challenges of Immersive Social Media, 2024, accessed 11 September 2025, p 4
[14] Adapted from Interaction Design Foundation, Beyond AR vs. VR: What is the Difference between AR vs. MR vs. VR vs. XR?, accessed 11 September 2025

[15] Adapted from Interaction Design Foundation, Beyond AR vs. VR: What is the Difference between AR vs. MR vs. VR vs. XR?, accessed 11 September 2025
[16] J Gray M Carter & B Egliston, Governing Social Virtual Reality: Preparing for the Content, Conduct and Design Challenges of Immersive Social Media, 2024, accessed 11 September, p 5
[17] For example, the World Economic Forum has described metaverses as a future persistent and interconnected virtual environment where social and economic elements mirror reality (World Economic Forum, 2023) and the Organisation for Economic Co-operation and Development (OECD) has defined them as immersive environments based on augmented reality (AR), virtual reality (VR), mixed reality (MR) and other extended reality (XR) technologies that enhance the realism of virtual experiences, blurring the lines between the physical and digital worlds (OECD, 2022). - I Hupont Torres et al, European Commission, Next Generation Virtual Worlds: Societal, Technological, Economic and Policy Challenges for the EU, July 2023, accessed 11 September 2025, p 14
[18] B Egliston, M Carter, K. E. Clark, Who will govern the metaverse? Examining governance initiatives for extended reality (XR) technologies, 29 January 2024, accessed 11 September 2025, p 2
[19] UST Global, What is haptics technology?, accessed 11 September 2025
[20] I Hupont Torres et al, European Commission, Next Generation Virtual Worlds: Societal, Technological, Economic and Policy Challenges for the EU, July 2023, accessed 11 September 2025, p 10. Augmented virtuality, shown in Figure 1, refers to immersive experiences that are further along the spectrum towards VR in comparison to AR. Augmented virtuality in this figure can be equated with mixed reality, as it is described in this paper.
[21] C Rincon & J Perez, Ada Lovelace Institute, What are immersive technologies?, 5 March 2025, accessed 11 September 2025
[22] Varmine, The Role of 3D Rendering in Virtual Reality and Augmented Reality, accessed 11 September 2025
[23] Ada Lovelace Institute, What are immersive technologies?, 5 Mach 2025, accessed 11 September 2025
[24] J Gray, M Carter & B Egliston, Governing Social Virtual Reality: Preparing for the Content, Conduct and Design Challenges of Immersive Social Media, 2024, p 5
[25] J Gray M Carter & B Egliston , Governing Social Virtual Reality: Preparing for the Content, Conduct and Design Challenges of Immersive Social Media, 2024, p 5
[26] Note Meta Ray-Ban AI glasses are considered smart glasses with integrated AI features rather than XR glasses. although it is reported that future iterations could be XR glasses. For example, see TechRadar, New Meta XR glasses again tipped to land later this year – well ahead of Apple's rumored AR glasses with Apple Intelligence, 29 April 2025, accessed 11 September 2025
[27] Note the Android XR glasses were yet to be released 11 September 2025.
[28] B Heller et al, Existing Law and Extended Reality: An edited volume of the 2023 symposium proceedings, Stanford University, 2024, accessed 11 September 2025, p 18
[29] Rock Paper Reality, O Sinai, How AI is Making Immersive Experiences More Powerful, 24 January 2024, accessed 11 September 2025
[30] Rathenau Instituut, Immersive technologies, 2023, accessed 11 September 2025, p 8; Also see European Parliament, Directorate General for Parliamentary Research Services, Tackling Deepfakes in European Policy, 30 July 2021, accessed 11 September 2025, p XIII, 32-33
[31] For a discussion of the benefits of XR, see Brittan Heller, Balancing Realities: Navigating the Benefits, Risks, and Policy Landscape of Extended Reality, Drexel Law Review, 17(1), accessed 11 September 2025, pp 111-115
[32] DRCF, Immersive Technologies Foresight Paper, December 2023, accessed 11 September 2025, p 2
[33] For example, see Zero Latency VR, Awaken what's within, accessed 11 September 2025
[34] Apple, Apple Vision Pro, accessed 11 September 2024
[35] L Flora, Brands look to VR e-commerce to replace the in-store experience, 21 April 2020, accessed 11 September 2025
[36] P Rao, Glossy, YouTube launches AR virtual try-on capabilities with Mac Cosmetics ,18 June 2019, accessed 11 September 2025
[37] European Commission, Extended reality: opportunities, success stories and challenges in health and education, 24 February 2023, accessed 11 September 2025, p 48

[38] D Hamilton et al, Immersive virtual reality as a pedagogical tool in education: A systematic literature review of quantitative learning outcomes and experimental design, 11 July 2020, accessed 11 September 2025, p 21
[39] Varjo, Insight session: Bridging neuroscience and XR for superpowering the human experience, 26 January 2023, accessed 11 September 2025
[40] I Hupont Torres et al, European Commission, Next Generation Virtual Worlds: Societal, Technological, Economic and Policy Challenges for the EU, July 2023, accessed 11 September 2025, p 14-15
[41] Meta, Connect 2021: Our vision for the metaverse, 28 October 2021, accessed 11 September 2025
[42] For example, see S Rose, The metaverse will be our slow death!' Is Facebook losing its $100bn gamble on virtual reality?, accessed 11 September 2025, The Guardian, 7 December 2022; J Schreier, Bloomberg, Companies are spending billions on a metaverse that makes no sense, 11 February 2022, accessed 11 September 2025
[43] J Mann, Business Insider, Meta's CTO said the metaverse could be a legendary misadventure if the company doesn't boost sales, leaked memo shows, 3 February 2025, accessed 11 September 2025
[44] Global Insight Services, Extended reality market, December 2024, accessed 11 September 2025
[45] Precedence Research, Extended Reality Market Size, Share, and Trends 2025 to 2034, 10 January 2025, accessed 11 September 2025
[46] Rathenau Instituut, Immersive technologies, 2023, accessed 11 September 2025, p 12
[47] UK DRCF, Immersive Technologies Foresight Paper, 13 December 2023, accessed 11 September 2025, p 2
[48] Varjo, Motion sickness in VR, accessed 18 February 2025, accessed 11 September 2025
[49] Brittan Heller, Balancing Realities: Navigating the Benefits, Risks, and Policy Landscape of Extended Reality, Drexel Law Review, 17(1), accessed 11 September 2025, p 119
[50] H Kao et al, Loka: A Cross-Platform Virtual Reality Streaming Framework for the Metaverse, 11 February 2025, accessed 11 September 2025
[51] M Casasnovas et al, Experimental Evaluation of Interactive Edge/Cloud Virtual Reality Gaming over Wi-Fi using Unity Render Streaming, 7 August 2024, accessed 11 September 2025, p1
[52] World Economic Forum, Interoperability in the metaverse, 18 January 2023, accessed 11 September 2025
[53] Apple, Apple Vision Pro, accessed 11 September 2025
[56] Adjustment for inflation (end-June 2008 to end-March 2025) based on Australian Bureau of Statistics, Consumer Price Index, Australia (March quarter 2025), 30 April 2025, accessed 11 September 2025
[55] For example, see M Bujić et al, International Journal of Human-Computer Studies, Effects of Immersive Media on Emotion and Memory: An Experiment Comparing Article, 360-video, and Virtual Reality, November 2023, accessed 11 September 2025, accessed 11 September 2025, p 8
[56] M Carter et al, Disability in the Metaverse, The University of Sydney, 30 September 2024, pp 6-7; B Egliston, K.E Clark, & M Carter, "My VR does not acknowledge me as a person": Is the metaverse leaving disabled users behind?, ABC, 14 July 2023, accessed 11 September 2025
[57] DP-REG, Working Paper 3: Examination of technology – Multimodal Foundation Models, accessed 11 September 2025, 19 August 2024
[58] eSafety, Tech Trends position paper: Immersive technologies, May 2025, accessed 11 September 2025, p 26
[59] Interpol, Grooming, radicalization and cyber-attacks: INTERPOL warns of 'Metacrime', 18 January 2024, p 12
[60] B Heller, Watching Androids Dream of Electric Sheep: Immersive technology, biometric psychography, and the law, Vanderbilt Journal of Entertainment and Technology Law, 23 (1), 2020
[61] OAIC, Children's Online Privacy Code | OAIC, 5 August 2025 (updated), accessed 11 September 2025, p.26
[62] B Heller, Watching Androids Dream of Electric Sheep: Immersive technology, biometric psychography, and the law, Vanderbilt Journal of Entertainment and Technology Law, 23 (1), 2020, accessed 11 September 2025

[63] B Heller, Watching Androids Dream of Electric Sheep: Immersive technology, biometric psychography, and the law, Vanderbilt Journal of Entertainment and Technology Law, 23 (1), 2020, accessed 11 September 2025
[64] Equivalent protections for financial products and services are included in the *Australian Securities and Investments Commission Act 2001*, enforced by the Australian Securities & Investment Commission.
[65] Australian Government, Department of the Treasury, Unfair trading practices – supplementary consultation paper, 2024, accessed 11 September 2025, p 4-5
[66] A. D. Souchet et al, A narrative review of immersive virtual reality's ergonomics and risks at the workplace: cybersickness, visual fatigue, muscular fatigue, acute stress, and mental overload, 2022, p 20
[67] Monash University, Safe Use of Immersive Technologies: Virtual Reality (VR), Augmented Reality (AR), Mixed Reality (MR) Guidelines, September 2022, accessed 11 September 2025, p 1
[68] European Agency for Safety and Health at Work, Digitalisation and occupational safety and health (OSH), 2019, accessed 11 September 2025, p 11
[69] Monash University, Safe Use of Immersive Technologies: Virtual Reality (VR), Augmented Reality (AR), Mixed Reality (MR) Guidelines, September 2022, accessed 11 September 2025, pp 1-2
[70] J Spivack & D Berrick, Wired, 27 September 2023, Immersive Tech Obscures Reality. AI Will Threaten It, 27 September 2023, accessed 11 September 2025; Regarding the use of MFMs in products and services raising concerns about misleading or deceptive conduct, see DP-REG, Working paper: Examination of technology: Multimodal Foundation Models, accessed 11 September 2025, p 10
[71] J O'Hagan et al, Augmenting People, Places & Media: The Societal Harms Posed by Everyday Augmented Reality, and the Case for Perceptual Human Rights (author version), MUM '23: Proceedings of the 22nd International Conference on Mobile and Ubiquitous Multimedia, 2023, accessed 11 September 2025, p 5
[72] H Hadan et al, Deceived by Immersion: A Systematic Analysis of Deceptive Design in Extended Reality, ACM Comput. Surv. 56, 10, Article 250, 2024, accessed 11 September 2025, p 17
[73] ACCC, Digital Platform Services Inquiry – Final Report (DRAFT), accessed 11 September 2025, p 339
[74] Wang et al, The Dark Side of Augmented Reality: Exploring Manipulative Designs in AR, 2023, accessed 11 September 2025, p 2
[75] UK DRCF, Immersive Technologies Foresight Paper, 13 December 2023, accessed 11 September 2025, p 17
[76] L Buck and R McDonnell, Security and Privacy in the Metaverse: The Threat of the Digital Human, 2022, accessed 11 September 2025, p 3
[77] Z Yang et al, Inception Attacks: Immersive Hijacking in Virtual Reality, 2024, accessed 11 September 2025, p 1-3
[78] Z Yang et al, Inception Attacks: Immersive Hijacking in Virtual Reality, 2024, accessed 11 September 2025, p 6-8
[79] Regarding scam advertisements on social media platforms, see The Guardian, Going, going, gone: Scam websites imitating famous brands are luring in victims on social media. What can be done?, 24 May 2025, accessed 11 September 2025
[80] B Heller, Watching Androids Dream of Electric Sheep: Immersive technology, biometric psychography, and the law, Vanderbilt Journal of Entertainment and Technology Law, 23 (1), 2020, accessed 11 September 2025; For further discussion of the phenomenon of immersive advertising, see B Heller and A Bar-Zeev, The Problems with Immersive Advertising: In AR?VR, Nobody Knows You're An Ad, Journal of Online Trust and Safety, 1(1), 2021, accessed 11 September 2025
[81] Hine, E., Rezende, I., Roberts, H. et al., Safety and Privacy in Immersive Extended Reality: An Analysis and Policy Recommendations, DISO 3, 33 (2024) p 33.
[82] UK DRCF, Immersive Technologies Foresight Paper, 13 December 2023, accessed 11 September 2025, p 12-13
[83]Competition and Markets Authority (CMA), Trends in Digital Markets: A CMA Horizon Scanning Report, 14 December 2023, accessed 11 September 2025, p 36
[84] CMA, Trends in Digital Markets: A CMA Horizon Scanning Report, 14 December 2023, accessed 11 September 2025, p 37

[85] CMA, Trends in Digital Markets: A CMA Horizon Scanning Report, 14 December 2023, accessed 11 September 2025, p 36; Also see, I. Hupont Torres et al, European Commission, JRC Science for Policy Report, 'Next Generation Virtual Worlds: Societal, Technological, Economic and Policy Challenges for the EU', accessed 11 September 2025, p 59-62
[86] CMA, Trends in Digital Markets: A CMA Horizon Scanning Report, 14 December 2023, accessed 11 September 2025, p 37
[87] UK DRCF, Immersive Technologies Foresight Paper, 13 December 2023, accessed 11 September 2025, p 20
[88] XR Safety Initiative Europe, Competition in Virtual Worlds, submission to European Commission Call for contributions on competition in virtual worlds, submitted 10 March 2024, accessed 11 September 2025
[89] J Vanian & A Capoot, CNBC, Meta's Reality Labs posts $5 billion loss in fourth quarter, 29 January 2025, accessed 11 September 2025
[90] I. Hupont Torres et al, European Commission, JRC Science for Policy Report, Next Generation Virtual Worlds: Societal, Technological, Economic and Policy Challenges for the EU, 3 July 2023, accessed 11 September 2025, p 61
[91] C Rincon & J Perez, Ada Lovelace Institute, What are immersive technologies?, 5 March 2025, accessed 11 September 2025
[92] CMA, Cloud services market investigation - Summary of provisional decision, 28 January 2025, accessed 11 September 2025, p 3
[93] ACCC, Compliance and enforcement priorities, 2025, accessed 11 September 2025. The ACCC's enduring priorities include anti-competitive conduct, product safety, consumers experiencing vulnerability or disadvantage, and scams.
[94] International Society for Computational Biology, Betting on Innovation: Emerging Technologies Revolutionizing Gambling, accessed 11 September 2025
[95] Family Addiction Specialist, A New Age of Digital Addiction - What The Metaverse Means for Mental Health and Digital Addiction : Family Addiction Specialist: Addiction Counselor, accessed 11 September 2025
[96] Venture Burn, Virtual and Augmented Reality: The New Reality of Betting, 27 May 2024, accessed 11 September 2025
[97] J Spivack & D Berrick, Wired, Immersive Tech Obscures Reality. AI Will Threaten It |, 27 September 2024, accessed 11 September 2025
[98] World Economic Forum, Metaverse interoperability is essential. How will regulation play a part?, 6 August 2024, accessed 11 September 2025
[99] Amplification of any content necessarily involves giving it preference over other content. By amplifying some content, recommender systems can end up deprioritising or excluding different viewpoints or valuable ideas contrary to a person's existing beliefs, contributing to what are commonly known as 'echo chambers'. eSafety's position statement on recommender systems and algorithms provides additional information, see eSafety Commissioner, Recommender systems and algorithms – position statement, December 2022, accessed 11 September 2025
[100] Australian Federal Police, Holiday season warning: Extremists infiltrating online and gaming platforms to recruit young Australians, 3 December 2023, , accessed 11 September 2025
[101] National Counterterrorism Innovation, Technology, and Education Center, Meta's Glasses, ChatGPT, and the Rise of High-Tech Extremist Violence, 8 January 2025, accessed 11 September 2025
[102] C Allen and V McIntosh, Limina Immersive commissioned by NSPCC, Child safeguarding and immersive technologies: An outline of the risks, September 2023, accessed 11 September 2025, p 22
[103] M Guggisberg, The Conversation, Virtual reality grooming is an increasing danger. How can parents keep children safe?, 1 February 2024, accessed 11 September 2025
[104] End-to-end encryption can prevent or limit the detection of online grooming or CSEA by blocking technologies that can identify illegal material and activity. For more information, refer to eSafety's position statement on end-to-end encryption, accessed 11 September 2025
[105] A Crawford, BBC, Child abuse material found on VR headsets, police data shows, 23 February 2023, , accessed 11 September 2025

[106] J O Bailey and J N Bailenson, Cognitive Development in Digital Contexts, 2017, page 186, accessed 11 September 2025
[107] B Kenwright, Virtual reality: ethical challenges and dangers [opinion], IEEE Technology and Society Magazine, 2018, accessed 11 September 2025
[108] R Sparrow and L Karas, Teledildonics and rape by deception, 2020, , accessed 11 September 2025
[109] eSafety, The metaverse: A snapshot of experiences in virtual reality, December 2023, page 17, accessed 11 September 2025
[110] A Powell, A Flynn, S Hindes, ANROWS, Technology-facilitated abuse: National survey of Australian daults' experiences, July 2022, accessed 11 September 2025
[111] J Outlaw, Virtual harassment: The social experience of 600+ regular virtual reality (VR) users, 4 April 2018, accessed 11 September 2025
[112] J E Gray, M Carter and B Egliston, Governing Social Virtual Reality: Preparing for the Content, Conduct and Design Challenges of Immersive Social Media, 2024, page 24
[113] The OSA provides for industry bodies or associations to develop codes to regulate certain types of seriously harmful online material, and for eSafety to register and enforce the codes. If the Commissioner is not satisfied that a Code meets the statutory requirements of the Act for registration, then eSafety may develop an industry standard for that section of the online industry instead. The industry bodies tasked with developing the industry codes adopted a two-phased approach, consistent with eSafety's guidance. The first phase targets the most seriously harmful class 1 material, which includes child sexual exploitation material, pro-terror material, and extreme crime and violence material. The second phase of industry codes development broadly focuses on children's access and exposure to class 2 material, which includes online pornography, and other high-impact themes.
[114] The Minimum Compliance Measures required under a code or standard vary in accordance with a service's risk tier and categorisation. More information on identifying the applicable code or standard, and how to comply with the relevant obligations, is available in eSafety's regulatory guidance on Phase 1 codes and Phase 1 standards.
[115] Australian Government, Department of the Treasury, Review of AI and the Australian Consumer Law, accessed 11 September 2025
[116] In addition, see Council of Europe and Institute of Electrical and Electronics Engineers, The Metaverse and its impact on human rights, the rule of law and democracy, May 2024, accessed 11 September 2025
[117] European Commission, Commission launches calls for contributions on competition in virtual worlds and generative AI, 9 January 2024, accessed 11 September 2025