STANDARDS Australia 100

CELEBRATING 100 YEARS 1922-2022

WHITEPAPER

The Metaverse and Standards

May 2023

ABOUT STANDARDS AUSTRALIA

Standards Australia is an independent, non-government, not for profit organisation. We are the nation's peak non-government standards development organisation.

The work of Standards Australia and our staff, stakeholders, members and contributors enhances the nation's economic efficiency, international competitiveness and contributes to a safe and sustainable environment for all Australians.

Standards Australia's vision is to be a global leader in trusted solutions that improve life – today and tomorrow.

Authors

The Metaverse Standards Whitepaper project was led by Dr Catriona Wallace, Founder of the Responsible and Metaverse Alliance (RMA).

Responsible Metaverse Alliance

The Responsible Metaverse Alliance (RMA) is a social enterprise and international movement dedicated to supporting the development of the metaverse, and virtual worlds, so that they are handled responsibly from a perspective of design, deployment, safety, culture, inclusion, operations and function. The RMA has a focus on working with politicians, government officials, regulators and policy makers internationally, to support them in addressing potential harms of the metaverse.

Dr Catriona Wallace

Dr Catriona Wallace is an AI and Metaverse specialist, with a focus on the responsible use of technology. Catriona has been recognised by AFR as the most influential woman in business and entrepreneurship and by Onalytica as one of the top speakers, globally, on both Ethical AI and the Metaverse. Catriona co-authored the book *Checkmate Humanity: the how and why of Responsible AI.*

An expert in Digital Transformation, Dr Wallace is the Founder of the Responsible Metaverse Alliance, an Adjunct Professor, and Chairs the Boab AI venture fund. Catriona was the Founder of a machine learning company based out of New York.

Dr Louis Rosenberg

Dr. Louis Rosenberg is an early pioneer of virtual and augmented reality. His work began over thirty years ago in VR labs at Stanford University and NASA. In 1992 he developed the first functional mixed reality system (Virtual Fixtures platform) at Air Force Research Laboratory. In 1993 he founded the early VR company Immersion Corporation which he brought public on NASDAQ in 1999. In 2004 he founded Outland Research, an early developer of geospatial augmented reality technology that was acquired by Google in 2011. He is currently Founder and Chief Scientist of Unanimous AI, a company that amplifies human intelligence in shared environments. Rosenberg received his PhD from Stanford University, was a tenured professor at California State University, and has been awarded over 300 patents for VR, AR, and AI technologies. He's currently CEO of Unanimous AI, the Chief Scientist of the Responsible Metaverse Alliance, and the Global Technology Advisor to XRSI.

Kavya Pearlman

Well known as the "Cyber Guardian," Kavya Pearlman is an award-winning cybersecurity professional and the founder & CEO of the XR Safety Initiative (XRSI), a Standard Developing Organization with the mission to help build safety and inclusion in emerging tech ecosystems. Kavya is the pioneer of the novel XRSI Privacy and Safety Framework for the Immersive Technologies Domain, Metaverse Safety Week Annual Awareness Campaign, and various baseline security, privacy and ethics standards for Emerging Technologies. She has won several awards for her work and been named one of the Top twenty Cybersecurity influencers for three consecutive years, 2018-2019-2020, and again for the year 2022 by IFSEC Global.

Kavya has previously advised Facebook on third-party security risks during the 2016 US presidential elections and worked as the head of security for the oldest virtual world, "Second Life" by Linden Lab. Kavya is the leading voice in cybersecurity, privacy, and Ethics for Emerging technologies including AR, VR, XR, exploring cross-sections of 5G, AI, and BCI - leading Standards development and promoting Diversity and Inclusion in the Immersive Technologies.

Kavya serves as the key member to Global Coalition for Digital Safety at the World Economic Forum (WEF) and a subject matter expert at several Security and safety focused multidisciplinary groups including INTERPOL's Metaverse Experts Group (i-MEG), United Nations Business and Human Rights Working Group, Metaverse Standard Forum, Responsible Metaverse Alliance and the new Metaverse Initiative at WEF. Kavya currently advises over 30 global governments and several big tech corporations on cybersecurity and global policymaking to safeguard humans in emerging tech ecosystems.

Bhanujeet Choudhary

Bhanujeet Choudhary is a strategist and visionary leader, with a passion for creating a sustainable future through emerging technologies. With over 7 years of experience in operations and technology, he currently serves as the Chief of Staff at XRSI, a global non-profit with a mission to build safety and inclusion in the immersive ecosystem. He is leading the charge in developing innovative, pragmatic and decentralized solutions with a deep understanding of privacy, statistics, economics, AI/ML, and organizational development.

Bhanu contributes to several efforts focused on building safe, open, interoperable Metaverse, including Metaverse Standards Forum and IEEE. He is also the Events Director for Metaverse Safety Week (MSW), a global awareness campaign to bring the world together for safeguarding the Metaverse.

We also wish to thank the Chair of the Metaverse Standards Forum, Neil Trevett for his support with this White Paper.

Acknowledgement

Standards Australia would like to acknowledge the support of the Australian Department of Industry, Science and Resources in the development of this white paper.

Contents

Executive Summary

- The Metaverse may be defined as, *"A network of interconnected virtual worlds with the following key characteristics: Presence, Persistence, Immersion and Interoperability. Metaverse is the next iteration of the internet enabled by several converging technologies such as Extended Reality (XR), Artificial Intelligence (AI), Decentralised Ledger Technologies (DLTs), neuro-technologies, optics, bio-sensing technologies, improved computer graphics, hardware, and network capabilities."* (XRSI)
- Additionally, the Metaverse may be described as, *"Persistent and immersive simulated worlds that are experienced in the first person by groups of simultaneous users who share a strong sense of mutual presence."* (Dr Louis Rosenberg)
- The Metaverse received over US$200 billion+ in investment in 2022 and has the potential to generate up to US$5 trillion in value by 2030 (McKinsey).
- Risks related to the Metaverse include Human Risks, Societal Risks, Regulatory Risks, Legal Risks, Information Risks, and Financial Risks. More specifically there are also User on User Risks, Bad Actors Risks, Corporate Abuse Risks and Psychological Wellbeing Risks.
- Those at risk from the Metaverse include children and young people, marginalised and disadvantaged communities, elderly, individuals with disabilities or health conditions and businesses and organisations.
- Currently, there are no specific regulations in place for the Metaverse. However, there are some existing laws and regulations that may apply to certain aspects of the Metaverse, such as data protection and privacy laws, intellectual property laws, and criminal laws.
- Organisations working on Metaverse Standards include: Metaverse Standards Forum, XRSI, World Wide Web Consortium (W3C), Virtual World Society, Computer Technology Association, Institute of Electrical and Electronics Engineers, International Organisation for Standardisation, International Telecommunication Union, Open Geospatial Consortium and the World Economic Forum.
- There are a number of existing regulatory frameworks, initiatives and standards-related bodies of work that exist in Australia that may be extended to the Metaverse. These include the Online Safety Act, the eSafety Commissioner's Safety by Design initiative, the Privacy Act, Immersive Technology Guidelines and Artificial Intelligence Ethics Framework
- Potential categories for Metaverse Standards include Security and Privacy; Accessibility standards; Content creation standards; Intellectual property standards; Governance and regulation standards; Ethical and moral standards, Interoperability standards and Child Safety Standards.
- Australia could build upon its existing work in the area of online safety and Safety by Design and extend this to **Standards to prevent targeted influence and manipulation in the Metaverse.** These standards should include:

    1. The Right to Experiential Authenticity
    2. The Right to Emotional Privacy
    3. The Right to Behavioural Privacy
    4. The Right to Human Agency

- Additional areas for Standards focus in Australia may be: Building Safety by Design into Metaverse standards; focusing on Responsible AI aspects of Metaverse platforms and extending the Responsible AI framework and Child Safety Standards.

Defining the Metaverse

Derivation of the term 'Metaverse'

"The Metaverse" is a marketing term popularised in the early 2020's by Meta [1] and derived from the 1990's science fiction novel Snow Crash [2]. It generally refers to the scientific disciplines of Virtual Reality (VR) and Augmented Reality (AR) with the caveat that it generally implies a significant social component such that multiple users can share experiences in virtual or augmented environments.

Potential definitions of Metaverse

There is no one widely accepted definition of the Metaverse. Even amongst our own team the thinking differs, particularly when we are considering the near term versus what we believe may be a longer-term construct of the Metaverse.

For some, the word Metaverse implies a fully immersive society with a working economy, however this is not generally accepted by academics as a requirement. Similarly, for some the word Metaverse is often conflated with specific infrastructure technologies such as Blockchain, Cryptocurrencies, NFTs and other decentralised forms of information storage and retrieval. While such pieces of infrastructure are employed by some developers of Metaverse technologies and may become popular, it is not considered a requirement.

Metaverse expert and VR pioneer, Chief Scientist for the Responsible Metaverse Alliance and CEO of Unanimous AI, Dr Louis Rosenberg notes that a working definition of Metaverse that aims to capture the essence of the concept without over constraining the concept to specific pieces of technical infrastructure or specific types of social and economic structures is as follows:

"The Metaverse refers to persistent and immersive simulated worlds that are experienced in the first person by groups of simultaneous users who share a strong sense of mutual presence." [3]

It's important to note that:

- Immersive worlds can be fully simulated (i.e., Virtual Worlds) or can be layers of virtual content overlaid on the real world (i.e., Augmented Worlds) [4]
- Mixed Reality (MR) is often used as a synonym for augmented reality but implies a more intimate mix of real and virtual content
- The phrase Extended Reality (XR) is often used to refer to the broad spectrum of immersive technologies including VR, AR, MR and sometimes telepresence [5].

One of the first Standard Developing Organizations to propose a standards definition of the Metaverse, XRSI defines the Metaverse as:

"A network of interconnected virtual worlds with the following key characteristics: Presence, Persistence, Immersion and Interoperability. Metaverse is the next iteration of the internet enabled by several converging technologies such as Extended Reality (XR), Artificial Intelligence (AI), Decentralised Ledger Technologies (DLTs), neuro-technologies, optics, bio-sensing technologies, improved computer graphics, hardware, and network capabilities."

Per the proposed standard definition, XRSI notes that the four key characteristics of the metaverse are as follows:

Presence. Presence refers to the feeling of being present or physically located within a digital environment. By simulating realistic sensory experiences and enabling participants to interact with objects and other individuals, it creates a sense of immersion and engagement within the virtual world as if they were in the same physical space.

Persistence. Persistence refers to the ability of virtual objects, environments, and experiences to persist over time, even when participants are not actively interacting with them. Persistence

allows participants to make progress, own virtual property, and build ongoing relationships, virtual worlds can provide individuals with a sense of investment and long-term engagement within the digital environment.

Immersion. Immersion refers to the degree to which an individual is fully engaged and absorbed in a virtual environment, to the point where the participant may forget about their physical surroundings. It can be achieved by creating an environment that feels believable and responsive to participant's actions and inputs, through the use of various technological and sensory inputs, such as virtual reality (VR) headsets, haptic feedback devices, and 3D audio.

Interoperability. Interoperability refers to the ability of different virtual worlds and systems to communicate and interact with each other seamlessly, allowing individuals to move freely between different digital environments and experiences. In the context of the Metaverse, interoperability is essential for creating a cohesive and interconnected virtual world that allows individuals to seamlessly move between different experiences and platforms.

Technologies that make up the Metaverse

The Metaverse is generally referred to as the next iteration of the Internet, that is persistent, shared and 3-dimensional. The Metaverse has been called the 'successor state' to mobile computing. Just as mobile phones didn't replace desktop computers, the Metaverse will increasingly come to dominate user time and attention, however, it may not replace the personal computers and mobile devices entirely. Instead of scrolling through mostly 2-dimensional screens, individuals will spend more and more of their time in digital experiences that are 3-dimensional, immersive, social, and increasingly indistinguishable from 'reality.' There are competing visions for the Metaverse, and regardless of the direction in which it evolves, both centralised and decentralised architectures will co-exist in competition.

The Metaverse will allow humans to Create, Connect, do Commerce, and have numerous applications and Use Cases including healthcare, education, gaming, entertainment, travel and construction via various converging technologies, as indicated in the following Figure 1: Anatomy of the Metaverse.

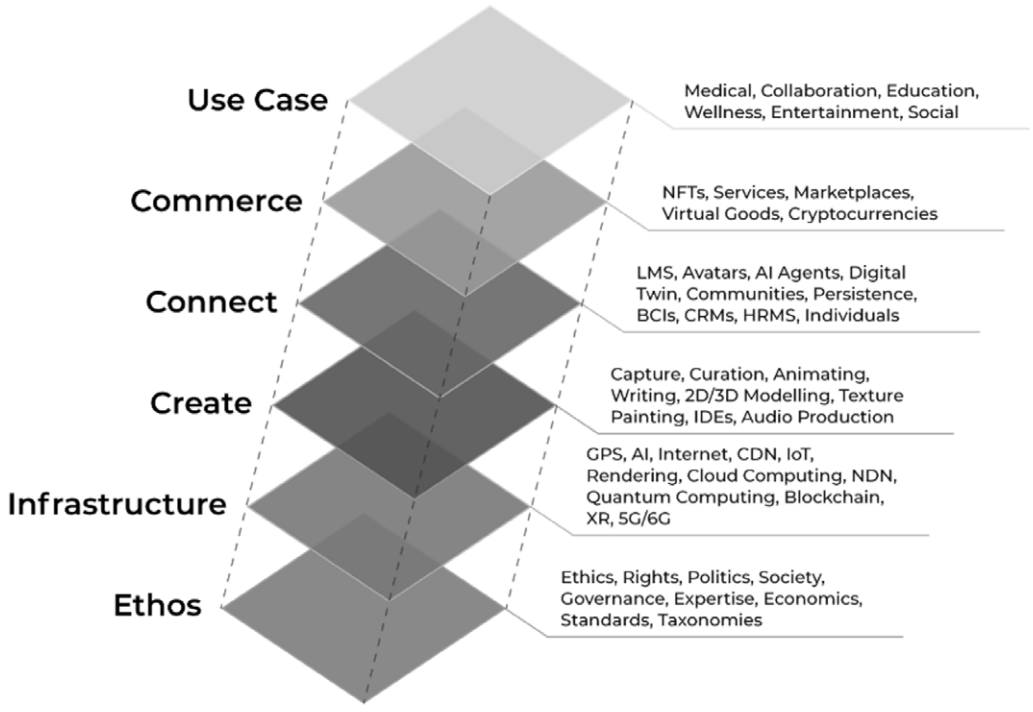

Fig 1: Anatomy of the Metaverse

A list of the key technologies that make up the construct of the Metaverse include the following (non-exhaustive) list:

1. Immersive Technologies
    a. Virtual Reality (VR)
    b. Augmented Reality (AR)
    c. Mixed Reality (MR)
    d. Volumetric Video Capture
    e. 360 Degree Video
    f. Haptics
2. Artificial Intelligence (AI)
    a. AI Agent, Machine Learning, Large Language Models, Chatbots
3. Neuro Technologies
    a. BCI (brain computer interface)
    b. Bio Sensors
4. Decentralised Ledger Technologies
    c. Blockchain, Hedera (fully open-source public distributed ledger), other
    d. NFT (non-fungible token)
5. Sensors
    e. Motion sensors, neural-sensors, eye-tracking sensors, haptic sensors, environmental sensors, audio sensors etc
6. Optics - Optics plays a critical role in building XR systems, enhancing the user's experience, and enabling the creation of lightweight and compact devices
    a. Lenses
    b. Lasers
    c. Holographs
7. Spatial Audio (3D Spatial Audio)

The list above is not a comprehensive list and as the Metaverse evolves, there will be numerous other technologies that converge to make up the immersive internet.

The size of the Metaverse

According to McKinsey & Co, the Metaverse received over US$200 billion+ in investment in 2022 and has the potential to generate up to US$5 trillion in value by 2030. They define the space as technologies and services that relate to 'immersive reality' and they specifically exclude from their calculations, the crypto market, blockchain, NFTs and other Web3 technologies that some influencers have incorrectly conflated with the definition of the Metaverse. On the other hand, McKinsey specifically includes immersive software applications that do not require VR or AR headsets [6]. From this perspective, two of the largest current Metaverse platforms are Roblox, which reportedly had over 58 million daily active users in 2022 and Fortnight which had over 20 million (neither of which call themselves Metaverse companies).

On the other hand, platforms that specifically claim to be Metaverse platforms have struggled greatly to gain traction. Meta's deeply funded Horizon World which aimed to achieve 500,000 daily active users in 2022 did not even reach 200,000. It is also reported that most users do not return after the first month [7]. Even more concerning for Metaverse proliferation, highly funded startups including Decentraland and Sandbox are believed to have had less than 1,000 daily active users in 2022, both of which have been tainted by their association with speculative NFTs [8]. The status and size of the Metaverse will likely change as Apple is predicted to launch their own Mixed Reality headset in late 2023 that the company expects will one day rival the iPhone in its market importance, lending a major vote of confidence to the view that immersive technologies will live up to their world-changing potential [9].

Australians' views on the Metaverse

Although there is currently no reliable data yet to estimate the value of the Metaverse to the Australian economy specifically, it is expected that this technology shift will have a significant impact on Australian society, economy and life.

Research by Capterra, published in December 2022, suggests that Australians are interested in the Metaverse with over half (57%) believing 'it is here to stay and will affect everyone's life to an extent'. Other key findings from the research of 1,001 respondents include:

- 30% of respondents said they 'knew exactly' what was meant by the term Metaverse
- 33% 'knew the name Metaverse but not the concept'; 17% were 'not familiar' with the term and 50% said they were unfamiliar with the concept.
- 39% of Aussies view the metaverse concept positively, whilst only 18% said they feel negative about it.
- Only 8% of survey-takers have accessed the metaverse,
- With regard to the use of the Metaverse, the most popular answers were:
    - Gaming (60%)
    - Attending virtual conferences/ events (39%)
    - Interacting with other people (38%)
    - Shopping for virtual products, such as avatar personalisation (34%)
    - Shopping for physical products, such as trying on clothes to buy later in real life (20%)

Disadvantages of the Metaverse noted by respondents were:

- Increased cybersecurity risks 48%
- Addiction to the virtual world 46%
- Personal data may be easily compromised 44%
- The equipment is expensive 42%
- Crimes could be hard to investigate 37%

It is clear that Australians are becoming aware of this next technology shift, with most believing it is here to stay, half being concerned about security and privacy and over a third being worried about crimes in the metaverse.

What the Metaverse is not

In defining what the Metaverse is, it is useful to identify what it is not. The Metaverse is not a single platform or application, limited to gaming, a replacement for the real world, or fully developed just yet. Additionally, the Metaverse is not the same thing as virtual reality platforms, augmented reality platforms, online games, social media platforms, or decentralised commerce platforms although it may include elements of these concepts.

Definitions of related fields that are sometimes confused or confounded with the concept of the Metaverse are set out below:

Virtual Reality (VR) platforms: Virtual Reality is a technology that allows individuals to experience immersive digital environments. However, VR platforms are not the same as the Metaverse, as the latter concept encompasses a much broader range of digital experiences beyond virtual reality. The Metaverse is not just limited to immersive environments, but also includes social interaction, cross platform interconnectivity, and much more. For example, the Oculus VR platform by Meta, is primarily a hardware and software platform for VR gaming and entertainment and does not offer the same level of interconnectedness and interoperability as a true Metaverse would.

Augmented Reality (AR) platforms: Augmented Reality technology overlays digital content onto the physical world to enhance the user's perception of reality and by providing additional information or virtual objects that are seamlessly integrated into the user's field of view. AR can be part of the Metaverse, but it is not the same thing as the Metaverse. For example, Pokémon Go is an AR game and does provide a sense of immersion, but it is not the Metaverse.

Online games: Online games like Fortnite or World of Warcraft are often mistaken for the Metaverse due to their virtual spaces and social interaction features. However, the Metaverse is not limited to online gaming experiences. It is a much larger concept that includes all types of digital experiences, from commerce to social interaction. Once the Metaverse is fully realised, Online games will remain a part of the Metaverse, however, to call an online game "the Metaverse" would be misleading. For example, Minecraft is a popular online game, but it is not the Metaverse.

Social media platforms: Social media platforms like Discord, Facebook or Twitter are not part of the Metaverse, although they may have virtual reality or augmented reality features. While social media allows for virtual social interaction, the Metaverse is a fully immersive virtual world that goes beyond just social interaction. The Metaverse includes user-generated content, virtual economies, and much more.

Decentralised commerce platforms: Decentralised commerce platforms use blockchain technology to create decentralised marketplaces, often referred to as web3 platforms, where individuals can buy and sell goods and services without intermediaries like banks or payment processors. While these platforms may be part of the Metaverse, they are not the same thing as the Metaverse. The Metaverse is a much larger concept that involves a fully immersive virtual world, whereas some platforms focus specifically on decentralised commerce. For example, OpenSea is a web 3 commerce platform for buying and selling NFTs, but it is not the Metaverse.

Closed virtual worlds and ecosystems: Closed ecosystems with limited interoperability are not considered the Metaverse because they lack the fundamental characteristic of an open, interconnected, and interoperable virtual world. They are typically closed ecosystems with limited interoperability, and they may have their own separate economies, currencies, and rules. Some of these closed virtual world ecosystems that are not the Metaverse include Second Life, Minecraft, Roblox, Sandbox, Animal Crossing, VRChat, IMVU, The Sims etc.

Main players in the Metaverse

The Metaverse will not be built by a single organisation.

The main players of the Metaverse will be determined by the companies enabling the Metaverse. These players will be from different domains including Hardware (Like Nvidia, Magic Leap, AMD, Meta, HTC, Snapdragon, Qualcomm, etc), Networking (Cloudflare, Huawei, AT&T, T-Mobile, Vodafone etc.) Compute (Amazon, Azure, Google, etc.), Virtual Platforms (Immerse, Bytedance's Pico Store, Oculus VR etc.), and Interchange Tools & Standards (Nvidia's Omniverse, Unity, Unreal, Gltf, etc)

The Metaverse is still a developing concept, and new players may emerge as the technology and market evolve. Overall, the key players in the Metaverse will be determined by the success of the enablers. Figure 2 below presents the core enabling components of the Metaverse.

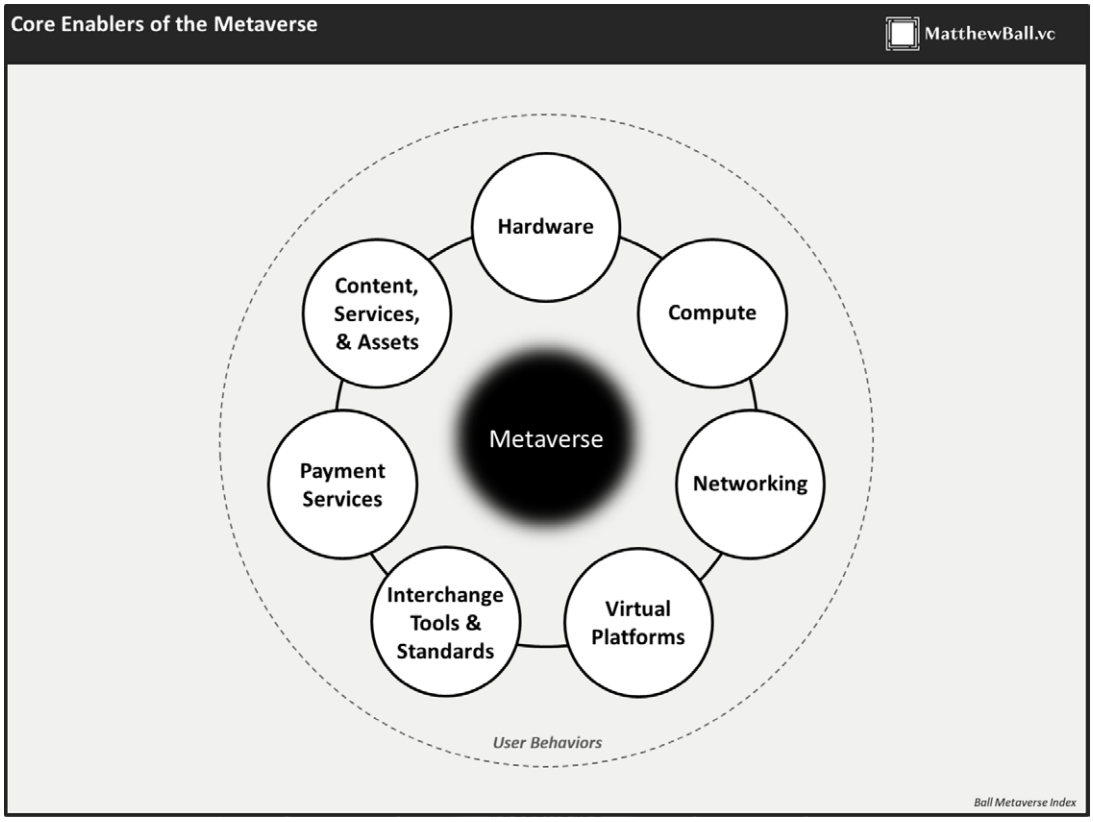

Figure 2: Core enablers of the Metaverse **(Matthew Ball)**

Some of the top Metaverse platform players, as noted by Technology Magazine, include (please see details of each platform in the Appendix):

1. Cryptovoxels
2. Unity Technologies
3. The Sandbox
4. Roblox
5. Decentraland
6. Epic Games
7. NVIDIA Omniverse
8. Microsoft Mesh
9. Meta Horizon Worlds
10. Niantic
11. Bytedance PICO

There are thought to be over 160 virtual worlds in existence. Hence it is important to recognise that the status of Metaverse platforms such as Meta's Horizon World is not representative of the Metaverse in its entirety. Additionally, it is not only the tech giants creating virtual worlds, there are also many startups focused in this area currently.

Some of the top Metaverse startups, as recognised by Start Us Insights are: (please see details in Appendix)

1. RLTY
2. Kirin Metaverse
3. Bit.Country
4. Edverse
5. landindex
6. Veyond Metaverse
7. Metaboutiq
8. Next Earth
9. Black History DAO
10. KEYS Metaverse

Therefore, we can see that the Metaverse is far more expansive than the few top players, such as Meta and Microsoft, hence we should be cautioned about making judgements on the status of the Metaverse based on the financial or other performance of only the top few Metaverse associated organisations.

The risks of the Metaverse

As described above, the Metaverse is enabled by the convergence of several technologies and characterised by immersive experiences in virtual and augmented worlds by creating a strong sense of mutual presence among the participating individuals. While there are many shared environments online today, from chat rooms, social media platforms, gaming, to online marketplaces, the Metaverse introduces a wide range of new risks. In the past, companies mainly concentrated on reducing financial, legal, and organizational risks. However, due to the convergence of various technologies, “immersive experiences”, and “mutual presence” the risks to “Humans in the loop” and “Societies in the loop” must be taken into account.[10]. By foreseeing these risks, we can take proactive measures to prevent harm to individuals, safeguard communities, and preserve ecosystems.

There are multiple ways to address and mitigate the risks associated with the Metaverse. One of the ways is to think about where the risks originate from. This is where the anatomy of the Metaverse can be a helpful way to establish whether the risk originates from a technology intersection, a specific use case, infrastructure, or the characteristics such as create, connect, commerce. Identifying the source of the risk will enable us to concentrate on preventive measures using tools like safety by design and establish regulatory and government models to provide concrete guidance to specific teams.

The root of these risks is the fact that first-person immersive experiences in virtual and augmented worlds can be extremely impactful on users, having psychological impacts that rival the real world [11]. This means users are significantly more affected by their experiences in the Metaverse as compared to other social environments. It also means that bad actors, corporate actors, state actors, and other third parties can impact users in far more personal ways in the Metaverse than traditional computing platforms [12].

The current and future risks related to the Metaverse can be further attributed into various categories including, Human Risks, Societal Risks, Regulatory Risks, Legal Risks, Information Risks, and Financial Risks. The actual risk could materialise into various concerns such as privacy, safety, payment integrity, compliance violation, data breach, identity issues, etc.

While the anatomy of the Metaverse provides the baseline to identify the source and establish a governance model following categories could be used to discover, analyse and mitigate these risks strategically:

Human Risks:
While humans represent themselves within the Metaverse as Avatars, the risks due to their presence are very real and can have real life consequences. These risks affect the safety and well-being of humans. The Metaverse could potentially lead to individuals experiencing addiction, social isolation, cyberbullying, identity theft, or psychological harm. Individuals may also face physical harm from using devices such as VR headsets or haptic suits that could malfunction or moving around hazardous surroundings could cause injuries.

Societal Risks:
The Metaverse will have a significant impact on society which could affect the social norms, values and cohesion of groups or communities. For example, the Metaverse could facilitate the spread of hate speech, and other harmful content, including, disinformation, misinformation, radicalization, polarisation etc while interacting with others in the metaverse.

Legal & Regulatory Risks:
Legal and regulatory risks can bring about significant challenges for the Metaverse as it evolves. While the regulatory risk will arise from the lack of governance, it could lead to legal uncertainty or liabilities. The legal risks could further result in disputes or lawsuits involving intellectual property, trademarks, copyright infringement, contractual disputes, etc. This is where XRSI

standards and frameworks could serve as a baseline to help navigate the legal and regulatory landscape in the Metaverse.

Information Risks:
These are risks that relate Confidentiality, Integrity, and Availability (CIA) of data and information generated by or exchanged within the metaverse. It involves the collection, processing, and storage of large amounts of data which could lead to data breaches, cyber-attacks, malware infections, privacy issues due to compromise of personal information or devices.

Financial Risks:
The Metaverse will involve a significant amount of financial investments. This could lead to financial risk such as, monetary losses or gains associated with the metaverse economy in the form of virtual real estate, virtual goods, virtual currencies, etc other forms of financial risks could include market and price volatility, taxation issues, regulatory changes, market crashes, competition, etc.

Building on these risk categories above, Dr Louis Rosenberg presents additional considerations for risks in the Metaverse. These include:

a. **User on User Risks** such as bullying and harassment,
b. **Bad Actors Risks** such as fraud and exploitation,
c. **Corporate Abuse Risks** such as predatory marketing and extreme privacy violations, and
d. **Psychological Wellbeing Risks** such as Metaverse addition and impacts to self-image. Each of these categories will be expanded in the section to follow.

User on User Risks:
In 2021, Pew Research reported that 41% of those surveyed have experienced some kind of online harassment on social platforms and that sexual harassment of women online has doubled since 2016 [13]. The problems are especially bad for teens. A 2022 Pew Research report found that nearly half of all American teens have been bullied or harassed online, with physical appearance being the most common reason why, especially among older teen girls [14]. These trends are likely to extend to the Metaverse and have the potential to be far more impactful in immersive worlds where the experiences are more direct, more realistic, and imparted as first-person experiences [11]. Already the London-based non-profit Center for Countering Digital Hate (CCDH), which monitors misinformation and harmful content online, has indicated that in VR Chat, a popular Metaverse platform, a user-on-user violation occurs about once every seven minutes [15].

In addition to harassment and bullying, other expected problems in the immersive worlds include hate-crimes, stalking, defamation, disparagement, and sextortion. When it comes to children and young adults, the Metaverse can be a very dangerous to venue, exposing kids to sexual predators who aim to groom, exploit, entice, or entrap them. This is particularly worrisome in fully immersive virtual worlds, as adults can easily pretend to be children of any age, gender, or nationality using avatars and voice cloning technology to lure kids into their confidence. A recent study conducted in VR Chat documented significant evidence of (i) minors being exposed to graphic sexual content, (ii) minors being exposed to sexual harassment, (iii) minors being conditioned repeat racist slurs and extremist talking points, (iv) threats of violence against minors [15]. Imran Ahmed, Chief Executive of the Center for Countering Digital Hate, said the study showed that some early Metaverse platforms are already “a haven for hate, pornography and child grooming.”

Bad Actor Risks:
A primary objective of immersive media technologies such as virtual and augmented reality is to fool the senses, making computer-generated content seem as authentic and interactive as real-world experiences. And while current generation platforms depict cartoonish avatars in game-like worlds, this will rapidly change, soon providing photorealistic experiences in very convincing

environments. And while the goal of fooling the senses is to provide users with magical experiences for everything from education and entertainment to shopping and fitness, bad actors will use the very same capabilities of the Metaverse to deceive, defraud, and exploit the public.

This is especially concerning now that AI technologies are able to generate simulated avatars that look, sound, and act like authentic people. In fact, a 2022 study by Lancaster University and UC Berkeley presented artificial human faces (i.e. photorealistic fakes) to hundreds of human subjects, along with a mix of real faces. They found that AI has become so effective, we humans can no longer tell the difference [16]. The researchers also asked their test subjects to rate the "trustworthiness" of each face. It turns out, people find the AI generated faces to be significantly more trustworthy [16]. This creates a very significant danger to the public, as bad actors will likely use friendly looking (and seemingly trustworthy) computer generated avatars to lure members of the public into deceptive, fraudulent, exploitive, and/or dangerous situations [17]. Most frightening, this will include bad actors using avatars that alter their perceived age and gender to target children.

In addition, deceptive tactics will include using avatars that accurately emulate the look and voice of people you know, luring you into conversations with a stranger with bad intentions. In this way, users could be targeted by bad actors posing as family members, co-workers, friends, schoolmates, or authority figures. In a 2022 blog post from Microsoft, Executive Vice President Charlie Bell said that fraud and phishing attacks in the Metaverse could "come from a familiar face – literally – like an avatar that impersonates your co-worker" and recommended that corporations prepare for such attack vectors [18]. These types of attacks could be used to extract company secrets as an insidious form of corporate espionage, fooling the target into thinking they are speaking with a member of their team. Similarly, these types of attacks could be used to extract bank information, fooling users into thinking they are sharing info with family members [19]. Already, fraudsters have begun using AI voice-cloning technology to emulate the voices of family members to scam people over the phone [20]. This will only get worse in the Metaverse.

Corporate Abuse Risks:
Based on current market trends, Metaverse platforms are likely to be developed and controlled by large corporate entities and will employ similar business models to those used by major social media platforms today. Considering the significant negative impacts that social media has had on democratic societies around the world, polarizing populations, driving extremism and propagating misinformation [21], we must consider if the Metaverse will pose similar dangers. Assuming these platforms adopt advertising-based business models similar to Facebook, Twitter, Instagram, and other large social platforms, we can expect that users will be tracked, profiled, and commoditized while using the Metaverse, ultimately becoming the regular targets of promotional influence campaigns. This might suggest that Metaverse platforms will could equally damaging to society as current social media, but the risks are actually far greater. That's because Metaverse platforms will be able to track, profile, and influence users in far more extensive and intimate ways.

> **Tracking and Profiling Users in the Metaverse:** Over the last decade, Big Tech has made a science of tracking, profiling, and commoditizing users on their platforms, enabling the sale of targeted ads. This has resulted in some of the most valuable corporations in human history. This business model has also made social media a polarizing force, allowing third parties to target specific political and/or demographic groups with content that amplifies existing biases and preconceptions, radicalising views, spreading misinformation, and amplifying discontent [22].
>
> In the Metaverse, platforms will not just track where users click and what they buy, but where they go, who they're with, what they do, what they look at, even how long their gaze lingers [3]. This will extend to the real world through augmented reality eyewear that tracks users as they walk down real streets in real towns, monitoring where they slow down and where they speed up, even recording which store windows they peer in and how long they

spend browsing. This will extend to users as they browse the aisles of real stores, visit restaurants and other establishments, and even track users in their own homes, schools, and workplaces. Metaverse eyewear will also track facial expressions, vocal inflections, and very likely certain vital signs (including blood pressure, heart rate, respiration rate, and pupil dilation) and will use this data to detect or infer real-time emotional states [23, 24, 25]. This combination of **behavioural tracking** and **emotional profiling** means that large Metaverse platforms will not just know how their users act throughout their day but will also be able to characterise how they feel during thousands of interactions, large and small, throughout their daily lives.

Targeted Influence in the Metaverse: For over 100 years, advertisers, politicians, and state actors have skillfully influenced the public using the mass media technologies of radio and then television. With the advent of social media, regional messaging has been transformed into **targeted messaging** that is aimed at a highly specific demographic category. This has greatly increased the persuasive impact, as third parties can now custom craft messaging for very specific groups and/or personal interests, values, and characteristics [26,27]. In the Metaverse, targeting will get significantly more personalized and the content will be **much** harder to identify as promotional material [28, 29]. That's because promotional material in the Metaverse will not be the pop-up ads and videos of today but will be immersive alterations to the user's spatial environment. This will include **Virtual Product Placements** (VPPs) that inject products, services and situations into a user's surroundings. This will also include promotional avatars, often referred to as virtual, humans or **Virtual Spokespeople** (VSPs) that will convey promotional material through conversational means that may seem like friendly banter.

Immersive advertising has the potential to be highly persuasive to the point of crossing the line from legitimate promotional tactics to predatory marketing. That's because without regulatory protection, users may not be able to distinguish between authentic aspects of virtual or augmented worlds and promotional artefacts that are injected specifically as targeted promotional experiences. In today's world we usually know when we're being marketed to and can muster a healthy dose of scepticism. In the Metaverse, this inherent layer of protection may no longer exist, as simulated people, products, and activities may be added to our reality without us knowing they were placed there for promotional purposes [12].

For example, in an unregulated Metaverse consumers will encounter "people" who look, act, sound and converse like any other user but are computer generated personas that are programmed to engage them in agenda-driven dialog that has a specific promotional objective. Even worse, these AI-powered avatars will have the ability to read facial expressions and vocal inflections, reacting to user's emotions in real-time. They will also be able to target us on a highly individualised level, armed with historical data about each user's personal traits, including our beliefs, interests, tendencies, and inclinations, plus a history of our previous interactions with similar agents. Sometimes referred to as the AI Manipulation Problem, we can also expect these conversational agents to optimize their influential tactics during real-time interactions, using AI-powered feedback loops to steadily adjust their persuasive approach based on our verbal responses and emotional reactions [31]. Unless regulated, such feedback loops could enable most persuasive form of targeted influence ever devised [32].

Psychological Wellbeing Risks:
According to the World Health Organization "Gaming Disorder" is a significant problem defined in the 11th Revision of the International Classification of Diseases (ICD-11) as a pattern of behaviour with respect to "digital-gaming" or "video-gaming" characterised by increased priority given to gaming over other daily activities and interests despite the occurrence of negative consequences [33]. Recent research suggests that virtual worlds, whether for traditional gaming or unstructured socialising can have similar addictive effects. A recent study performed by Rui Chen, Professor

of the Communication University of China, found VR games evoke a 20% higher “excitement level” than traditional gaming and that VR gaming environments are 44% more addictive than flat environments [34]. Other studies have found similar concerns about VR addiction [35].

> Augmented Reality is also causing psychological harm. At the present time, the most popular use of augmented reality technologies are face filters on social media platforms like Snapchat and TikTok. Young people, especially teenage girls, are using these filters to “beautify” their appearance by reshaping, recolouring, and enhancing their faces and bodies. This is causing significant “body dysmorphia” psychological harm and it’s currently happening entirely on the small flat screens of handheld phones [36]. As these capabilities transform into immersive 3D worlds, this harm is likely to get far, far worse.

The Metaverse related risks depend on the context which is derived from the use cases, stakeholders and the technologies involved. As we think about the risks the context is determined by the applications, stakeholders, functionalities and the technical intersection. For example, Second Life, is a 3D massive multiplayer virtual world incurs the possible risks of malicious codes, social engineering, frauds, harassment, etc. As the players interact with each other to create, connect and do commerce.

The risk categories discussed above are not exhaustive nor mutually exclusive however they illustrate some of the potential challenges and opportunities that await us as we enter into this new digital frontier.

Those at risk from the Metaverse

The Metaverse will have an impact on everyone, irrespective of their active participation level. However, certain groups may be more vulnerable or at higher risk, including:

Children and young people who may benefit from new forms of education, entertainment, and socialisation, but also face risks such as addiction, cyberbullying, and exposure to inappropriate or harmful content.

Marginalised and disadvantaged communities who may find new ways to express themselves, connect with others, and access resources and services, but also encounter discrimination, exclusion, and inequality in terms of access and opportunity.

Elderly, Individuals with disabilities or health conditions who may enjoy greater accessibility and inclusion in the Metaverse, but also face potential barriers to participation and access to support.

Businesses and organisations who may leverage the Metaverse to create new products, services, markets, and experiences for their customers and employees. But they also need to adapt to changing consumer preferences. And they need to compete with new entrants. And they need to comply with emerging regulations.

There may be several other risks that we may not have conceived yet. These are primarily phenomena that we may encounter as individuals or societies as a result of exposure and convergence of technologies. For example, hyper realistic virtual environments could lead to distorted perception of reality in adults and especially in children. Just like misinformation using traditional media the Metaverse can produce mis-experiences and potentially manipulate humans at mass scale. More research is needed to ascertain the future risks.

Existing work on Standards

Currently, there are no specific regulations in place for the Metaverse. However, there are some existing laws and regulations that may apply to certain aspects of the Metaverse, such as data protection and privacy laws, intellectual property laws, and criminal laws.

For example, many countries have data protection and privacy laws that apply to the collection, storage, and use of personal data, which could apply to the collection and use of data in the Metaverse. Intellectual property laws, such as copyright and trademark laws, could also apply to the creation and use of virtual content and assets in the Metaverse.

Additionally, criminal laws could be applied to certain activities in the metaverse that are illegal in the physical world, such as virtual sexual offences or the sale of virtual drugs or weapons. However, the application of these laws to the Metaverse may be complex and challenging, as the Metaverse is a virtual environment that operates differently from the physical and digital Web2.0 worlds.

As the Metaverse continues to evolve and expand, new standards and regulations and laws must be developed to address the unique challenges and opportunities presented by this technology.

Globally, there are a number of organisations working in the area of Standards for the Metaverse. These include the following:

Metaverse Standards Forum (MSF)

Hosted by the Khronos Group, the MSF membership is open, at no cost, to for-profit or non-profit organisations, including companies, standards organisations, industry associations or universities at no charge.

The MSF, with 2400 member organisations as of March 2023, states that they provide a venue for cooperation between standards organisations and companies to foster the development of interoperability standards for an open and inclusive Metaverse, and accelerate their development and deployment through pragmatic, action-based projects.

The MSF focuses on pragmatic, action-based projects such as implementation prototyping, hackathons, plugfests, and open-source tooling to accelerate the testing and adoption of standards, while also developing consistent terminology and deployment guidelines.

The activities of the MSF are directed by the needs and interests of its members and may involve diverse technology domains, including but not limited to:

- Interactive 3D assets and photorealistic rendering
- Human interface and interaction paradigms including AR, VR and XR
- User created content
- Avatars, identity management and privacy
- Financial transactions
- IOT and digital twins
- Geospatial systems

The MSF establishes pipeline of exploratory and domain working groups that meet regularly to create Charters and execute the projects they define.

The Working Groups as of March 2023 include:

- 3D Asset Interoperability using USD and glTF
- Digital Asset Management
- Metaverse Standards Register
- Real/Virtual World Integration

The Exploratory Groups currently include:

- Digital Fashion Wearables for Avatars
- Interoperable Characters/Avatars
- Network Requirements and Capabilities
- Privacy, Cybersecurity & Identity'
- Technical Interoperability and End-User Troubleshooting

XRSI

XR Safety Initiative (XRSI) is a 501(c)(3) global non-profit Standards Developing Organization (SDO) that offers advisory services to promote privacy, security, and ethics with a mission to help build safe and inclusive experiences. Headquartered in San Francisco Bay Area, XRSI currently advises over 30 governments and has over 200 diverse and multidisciplinary advisors from around the globe. XRSI is first such global effort and uniquely positioned to provide impartial, practical information about XR, emerging technologies and Metaverse-related risks and opportunities to individuals, corporations, universities, government agencies, and other organizations worldwide.

XRSI launched the first novel XRSI Privacy Framework for the XR domain to address the Privacy and Safety Issues in the Metaverse. XRSI has developed the immersive technology standards for accessibility, ethics, inclusion and safety. XRSI is currently working on Medical XR and Child Safety frameworks for addressing Privacy and Safety Issues in the Metaverse.

Since 2019, XRSI has created various programs focusing on the most critical aspects of the immersive domain, such as Medical XR (Medical XR Advisory Council), Child Safety (Child Safety Initiative), Diversity and Inclusion (CyberXR Coalition), Trustworthy Media Platform (Ready Hacker One), and the Metaverse Reality Check (The MRC), an oversight board by and for the citizens. XRSI is a member of the World Economic Forum (WEF) Global Coalition of Digital Safety as well as part of the Metaverse Initiative by WEF. XRSI provides contributions and oversight to several key open-source efforts pertaining to Metaverse-related technologies, including International Telecommunication Union (ITU), The Metaverse Standard Forum and Responsible Metaverse Alliance.

Open Metaverse Interoperability Group (OMG)

The OMG is an open, vendor-neutral group that aims to develop interoperability standards for the Metaverse. The group's focus is on developing open, transparent, and community-driven standards for virtual worlds, social networks, and other related technologies.

World Wide Web Consortium (W3C)

The W3C is an international community that develops standards for the web, including standards related to virtual and augmented reality. The W3C's WebXR working group is working on developing standards for immersive web experiences, including virtual and augmented reality.

Virtual World Society

The Virtual World Society is a non-profit organisation that aims to promote the use of virtual worlds and related technologies for social good. The organization is working on developing standards for virtual worlds that prioritize accessibility, education, and social responsibility.

Other organisations that are looking at potential standards for the Metaverse include:

- Computer Technology Association
- Institute of Electrical and Electronics Engineers
- International Organisation for Standardisation
- International Telecommunication Union
- Open Geospatial Consortium
- World Economic Forum

Thus, there are many organisations starting to look at Standards yet there is no one overarching, internationally agreed to and distributed set of Metaverse Standards.

Existing Standards, policy and legislation in Australia

There are a number of existing standards-related bodies of work, legislation and government initiatives that exist in Australia that may be extended to the Metaverse. These include:

The Online Safety Act

The Online Safety Act which came into effect in January 2022 expanded the abilities and powers of eSafety previously legislated in the Enhancing Online Safety for Children Act of 2015. The Act aims to improve and promote online safety for all Australians and covers topics such as:

- Cyberbullying
- Adult cyber abuse
- Image-based abuse
- Illegal content
- Harmful content
- Abhorrent violent material

The Online Safety Act:

- creates a world-first Adult Cyber Abuse Scheme for Australians 18 years and older, across a wide range of online services and platforms
- broadens the Cyberbullying Scheme for children to capture harms that occur on services other than social media
- updates the Image-Based Abuse Scheme to address the sharing and threatened sharing of intimate images without the consent of the person shown
- gives eSafety new powers to require internet service providers to block access to material showing abhorrent violent conduct such as terrorist acts
- gives the existing Online Content Scheme new powers to regulate illegal and restricted content no matter where it's hosted
- brings app distribution services and search engines into the remit of the new Online Content Scheme
- introduces Basic Online Safety Expectations for online service providers
- halves the time that online service providers have to respond to an eSafety removal notice, though eSafety can extend the new 24-hour period.

Safety by Design

Also led by eSafety is work on the Safety by Design initiative. Safety by Design, which puts user safety and rights at the centre of the design and development of online products and services, provides principles and guidance materials which may be extended to include the Metaverse and currently consists of:

- a set of **principles** that position user safety as a fundamental design consideration
- interactive **assessment tools** for mid-tier, enterprise and start up technology companies
- resources for **investors and financial entities**
- engagement with the **tertiary education sector** to embed Safety by Design into curricula around the world
- a youth vision statement, which was developed by young people, and details the expectations of children and young people of technology services and platforms
- ongoing engagement with industry and broader stakeholders from across the digital ecosystem

Safety by Design includes three core principles:

1. Service provider responsibility

The burden of safety should never fall solely upon the user. Every attempt must be made to ensure that online harms are understood, assessed and addressed in the design and provision of online platforms and services.

This involves assessing the potential risks of online interactions upfront and taking active steps to engineer out potential misuse, reducing people's exposure to harms.

To help ensure that known and anticipated harms have been evaluated in the design and provision of an online platform or service, the following steps should be taken:

1. Nominate individuals or teams and make them accountable for user safety policy creation, evaluation, implementation and operations.
2. Develop community guidelines, terms of service and moderation procedures that are fairly and consistently implemented.
3. Put in place infrastructure that supports internal and external triaging, clear escalation pathways and reporting on all user safety concerns, alongside readily accessible mechanisms for users to flag and report concerns and violations at the point they occur.
4. Ensure there are clear internal protocols for engaging with law enforcement, support services and illegal content hotlines.
5. Put processes in place to detect, surface, flag and remove illegal and harmful behaviour, contact and content with the aim of preventing harms before they occur.
6. Prepare documented risk management and impact assessments to assess and remediate any potential online harms that could be enabled or facilitated by the product or service.
7. Implement social contracts at the point of registration. These outline the duties and responsibilities of the service, user and third parties for the safety of all users.
8. Consider security by design, privacy by design and user safety considerations which are balanced when securing the ongoing confidentiality, integrity, and availability of personal data and information.

2. User empowerment and autonomy

The dignity of users is of central importance. Products and services should align with the best interests of users.

This principle speaks to the dignity of users, and the need to design features and functionality that preserve fundamental consumer and human rights. This means understanding that abuse can be intersectional, impacting on a user in multiple ways for multiple reasons, and that technology can deepen societal inequalities. To combat this, platforms and services need to engage in meaningful consultation with diverse and at-risk groups, to ensure their features and functions are accessible to all.

To help ensure that features, functionality and an inclusive design approach give users a level of empowerment and autonomy that supports safe online interactions, the following steps should be taken:

1. Provide technical measures and tools that adequately allow users to manage their own safety, and that are set to the most secure privacy and safety levels by default.
2. Establish clear protocols and consequences for service violations that serve as meaningful deterrents and reflect the values and expectations of the users.
3. Leverage the use of technical features to mitigate risks and harms, which can be flagged to users at relevant points in the service, and which prompt and optimise safer interactions.
4. Provide built-in support functions and feedback loops for users that inform users on the status of their reports, what outcomes have been taken and offer an opportunity for appeal.
5. Evaluate all design and function features to ensure that risk factors for all users – particularly for those with distinct characteristics and capabilities –have been mitigated before products or features are released to the public.

3. Transparency and accountability

Transparency and accountability are hallmarks of a robust approach to safety. They not only provide assurances that platforms and services are operating according to their published safety objectives, but also assist in educating and empowering users about steps they can take to address safety concerns.

The publication of information relating to how companies are enforcing their own policies and data on the efficacy of safety features or innovations will allow accurate assessment of what is working. If interventions are improving safety outcomes for users or deterring online abuse, these innovations should be shared and more widely adopted.

To enhance user trust, awareness and understanding of the importance of user safety, platforms and services should:

1. Embed user safety considerations, training and practices into the roles, functions and working practices of all individuals who work with, for, or on behalf of the product or service.
2. Ensure that user safety policies, terms and conditions, community guidelines and processes about user safety are accessible, easy to find, regularly updated and easy to understand. Users should be periodically reminded of these policies and proactively notified of changes or updates through targeted in-service communications.
3. Carry out open engagement with a wide userbase, including experts and key stakeholders, on the development, interpretation and application of safety standards and their effectiveness or appropriateness.
4. Publish an annual assessment of reported abuses on the service, alongside the open publication of meaningful analysis of metrics such as abuse data and reports, the effectiveness of moderation efforts and the extent to which community guidelines and terms of service are being satisfied through enforcement metrics.
5. Commit to consistently innovate and invest in safety-enhancing technologies on an ongoing basis and collaborate and share with others safety-enhancing tools, best practices, processes and technologies.

The Privacy Act 1988

The Privacy Act 1988 protects an individual's personal information regardless of their age. Australia has a strong track record in developing and implementing privacy and data protection laws. The country's Privacy Act, which regulates the handling of personal information by Australian government agencies and organisations, is widely regarded as one of the most comprehensive privacy laws in the world. Australia's experience in developing and implementing such laws could be leveraged in developing standards for data protection and privacy in the metaverse. https://www.legislation.gov.au/Details/C2014C00076

Immersive Technology Policy

An Immersive technology position statement has been published by eSafety. Additional Tech Trends and Challenges position statements available include related topics such as decentralisation, anonymity and identity shielding, doxing, deepfakes and recommender systems and algorithms.

Blockchain and Cryptocurrency Regulation

On 22 August 2022, the Government announced 'token mapping' – a foundational step in the Government's multistage reform agenda that commits to developing appropriate regulatory settings for the crypto sector. Token mapping seeks to build a shared understanding of crypto assets in the Australian financial services regulatory context. This will explore how existing regulation applies to the crypto sector and inform future policy choices.

Critical and Emerging Technologies standards

Standards Australia has partnered with the Australian Government's Department of Foreign Affairs and Trade on a two-year project to build knowledge and practical skills to support Critical and Emerging Technologies standards development in South-East Asia through a range of bilateral and regional activities. With an agreement signed May 2022, the project - International Standards Integration for Critical and Emerging Technologies in South-East Asia - launched in August 2022 and will conclude in June 2024.

Artificial Intelligence Ethics Framework

The Artificial Intelligence (AI) Ethics Framework guides businesses and governments to responsibly design, develop and implement AI. It's part of the Australian Government's commitment to make Australia a global leader in responsible and inclusive AI. For Australia to realise the immense potential of AI we need to be able to trust it is safe, secure and reliable.

Australia has a strong reputation internationally for its online safety legislation, and the Online Safety Act applied to foundational metaverse environments and platforms. As such, it is strongly recommended that the existing legislation and regulations are extended in scope to include the Metaverse.

The opportunities for Australia to develop Metaverse Standards

Research demonstrates that Australia has one of the highest online penetration rates in the world at 91% in 2022. This provides a large potential user base for Metaverse technologies and applications and also means that the Australian government and Standards organisations must enact standards and regulations in order to keep its citizens safe.

Australia also is one of the few countries that has exercised its regulatory powers to hold big technology companies accountable and protect citizens rights. As the Metaverse legal and regulatory landscape evolves, Australia can potentially provide policy guidance, standards and frameworks to establish a baseline of acceptable behaviours related to privacy, safety, security, ethics, inclusion, governance and shared responsibility.

Potential Standards categories

A number of potential categories for Metaverse Standards exist. These include:

Security and Privacy are critical concerns in the metaverse. Users will likely share a significant amount of personal and sensitive data in the metaverse, such as location, financial information, and personal preferences. As such, standards must be developed to ensure that users' data and identities are protected and that the platform is secure from cyber-attacks.

Security standards could include protocols for secure data transfer, encryption, firewalls, and intrusion detection systems. Privacy standards could include data collection policies, data retention policies, and user access controls.

Accessibility standards are essential to ensure that the metaverse is inclusive and accessible to all users, regardless of their physical abilities. This could include standards for text-to-speech and speech-to-text conversion, captioning, and assistive technology integration.

Additionally, accessibility standards could cover navigation, user interfaces, and platform features to ensure that users with disabilities can interact with the metaverse effectively.

Content creation standards refer to the ethical and responsible creation of user-generated content in the metaverse. This could include standards for acceptable use policies, moderation, and content review processes. Content creation standards could also cover the ownership and licensing of user-generated content, ensuring that creators retain appropriate rights, and that copyrighted content is appropriately licensed or attributed.

Intellectual property standards are critical to protecting creators' rights in the metaverse. This could include standards for copyright, trademarks, and patents, as well as protocols for intellectual property enforcement and dispute resolution. Additionally, intellectual property standards could cover content attribution and licensing to ensure that creators are credited for their work and that others do not use their work without permission.

Governance and regulation standards refer to the regulatory framework required to ensure that the metaverse operates fairly, transparently, and in compliance with relevant laws and regulations. This could include standards for user data protection, user privacy, and platform accountability. Governance and regulation standards could also cover platform transparency, such as publishing regular reports on content moderation, user data usage, and community guidelines enforcement.

Ethical and moral standards are essential to ensure that the metaverse operates ethically and responsibly. This could include standards for user conduct, community guidelines, and ethical use policies. Additionally, ethical and moral standards could cover issues related to social responsibility, such as the impact of the metaverse on society, and the potential for the

metaverse to promote positive change. This could include standards for diversity, equity, and inclusion, as well as environmental sustainability.

Interoperability standards refer to the ability of different components of the metaverse to work together seamlessly. This is important because the metaverse will likely be composed of various platforms, technologies, and services that need to communicate and exchange data. Without interoperability standards, different components may not be able to communicate effectively, which could limit the overall functionality and potential of the metaverse. Interoperability standards could cover a range of areas, including communication protocols, data formats, and APIs. They could also include standards for data privacy, security, and user authentication to ensure that data is shared safely and securely.

Child Safety

Possibly the most important area to consider standards for in Australia is the protection of children. Potential standards that could be put in place to ensure the safety and well-being of Australian children in the metaverse:

Age Verification Standards: Age verification is essential to prevent children from accessing age-inappropriate content or services. Age verification standards should require metaverse platforms to verify the age of users to ensure that children cannot access age-restricted content or services.

Content Moderation Standards: Content moderation is crucial to preventing children from being exposed to harmful or inappropriate content. Content moderation standards should require metaverse platforms to have robust content moderation systems in place, including AI-powered systems and human moderators, to detect and remove inappropriate content.

User Reporting Standards: User reporting is an important tool for users, including children, to report inappropriate behaviour or content. User reporting standards should require metaverse platforms to have clear and easy-to-use reporting mechanisms in place for users to report inappropriate content, behaviour, or users.

Parental Control Standards: Parental controls are essential to allow parents to monitor and control their children's activities in the metaverse. Parental control standards should require metaverse platforms to have robust parental control features that allow parents to set usage limits, filter content, and monitor their children's activities.

Education and Awareness Standards: Education and awareness are essential to help children and their parents understand the potential risks and challenges of the metaverse. Education and awareness standards should require metaverse platforms to provide clear and comprehensive guidance on safety, privacy, and security for children and their parents.

Data Protection Standards: Data protection is critical to ensure that children's personal information is protected and not misused. Data protection standards should require metaverse platforms to have robust data protection measures in place to ensure that children's personal information is kept safe and secure.

Access Control Standards: Access control is important to prevent unauthorised access to children's accounts or profiles. Access control standards should require metaverse platforms to have strong access control measures in place, such as two-factor authentication and password strength requirements.

Additionally, the Metaverse Standards Forum notes a register of potential areas that Standards may apply including:

1. Privacy, Safety, Security, Inclusion
2. Ethics, Privacy, Accessibility, Safety
3. Moral and Ethics Framework
4. Inclusive Design standards
5. Metaverse & The City (Global collaboration between governments)
6. Content Classification (Parental Control for Kids / Content Control for Adults)
7. Accessibility, User Experience
8. Inclusive Design standards
9. Default to Accessible
10. Embedded mechanism to know if you're interacting with a human or an algorithm
11. TAII Framework (Trustworthy Artificial Intelligence Implementation)
12. Shared Responsibility Model for Personal Safety
13. Define fundamental relationships and processes for lawful data processing in the metaverse
14. The application of privacy and data protection rights in the Metaverse
15. Icons to communicate different forms of processing activity
16. Evaluating Data Protection Impact Assessments in the context of the Metaverse
17. Exploring the demand for an industry "code of conduct" as per the GDPR
18. Responsible Metaverse Best Practice for developers, creatives and suppliers to the metaverse
19. Universal kick/boot framework thoughts Laws, such as the GDPR
20. UI and UX
21. Health and Medical
22. Geospatial protocols
23. Payment and economy protocols
24. Runtime and Object model
25. Governance and Advocacy
26. Video broadcasting and meetings
27. Tooling and creators
28. Performance and scalability
29. Gaming
30. Business analytics
31. Teaching, education and certification
32. Interoperable 3D assets
33. Real/Virtual world integration
34. Identity
35. Avatars and apparel

As the Metaverse can be regarded as the confluence of many technologies and attempts to emulate the physical and digital worlds plus introduces new experiences, capabilities, operations and functionality – then the full list of required Standards will be very large. As it is early days for Standards for the Metaverse, Australia is in a strong position to carve out a particular area of Standards expertise and lead the world in this regard.

Recommended areas of Metaverse Standards for Australia

As noted in this paper, there is a large number of areas where standards, policy and regulation are required for a safe and responsible Metaverse. However, for Australia to become a leader in the field of standards for the Metaverse, it is recommended that the nation builds upon its existing work in the area of **online safety** and the **Safety by Design** initiative – including three overarching principles – and extend this to one of the foundation components of the Metaverse, which is the ability of Metaverse platform providers to **target and manipulate users.**

It is the authors' recommendation that Australia focus on Standards to prevent targeted influence and manipulation in the Metaverse.

Standards and regulation to prevent targeted influence and manipulation

As described above, extensive tracking and profiling of users by Big Tech (and state actors) is well known among regulators. In the Metaverse, however, the magnitude and intimacy of consumer monitoring is likely to expand profoundly. Similarly, aggressive marketing and propaganda are not new problems faced by regulators, but in the Metaverse, users could find it difficult to distinguish between authentic experiences that they serendipitously encounter and targeted promotional content that is injected by a third party. For these reasons, policymakers must explore unique regulations that address these new risks. One way to think about the regulatory objectives is to guarantee basic "Immersive Rights" for citizens. At a minimum, the following rights should be considered:

1. The Right to Experiential Authenticity

CONTEXT:
At the present time, marketing is everywhere in our physical and digital worlds. That said, most adults can easily identify promotional content across a wide range of contexts. This allows individuals to view ads from the proper perspective – as paid messaging delivered by a party attempting to influence them. Having this context enables consumers to bring scepticism and critical thinking when considering messaging for products, services, political ideas, and other promotional content they are exposed to. In the Metaverse, advertisers could undermine our ability to contextualise promotional content by blurring the boundaries between authentic encounters and promotional experiences injected on behalf of paying sponsors (or state actors).

STANDARDS OR REGULATION:
To safeguard the public, policymakers should consider protecting a basic right to authentic experiences. This could be achieved by **requiring that all promotional artifacts in the Metaverse and all virtual spokespeople be visually and audibly distinct, enabling users to easily recognize them in the proper context** [3, 5, 12]. This would protect members of the public from mistaking promotionally altered experiences as authentic encounters.

2. The Right to Emotional Privacy

CONTEXT:
We humans evolved to communicate through highly expressive emotions on faces, voices, posture and gestures. Humans also evolved the refined ability to read such traits from others. This is a basic form of human communication that works in parallel with verbal language. Recently, sensing technologies combined with machine learning (ML) have enabled software systems to identify human emotions from our faces, voices, and bodies as well as from vital signs such as respiration rate, pupil dilation, heart rate and blood pressure. While this enables computers to engage in non-verbal language with humans,

it can be a major privacy concern. That's because AI systems can detect emotions from cues that are not perceptible to humans. For example, a human observer cannot easily detect heart rate, respiration rate, and blood pressure, which means those signals may be revealing emotions that the observed individual had not intended to convey. AI systems can also detect "micro-expressions" on faces that are too brief or too subtle for human observers to notice, again revealing emotions that the observed had not intended. Even more concerning, conversational agents could be designed to adjust their promotional tactics mid-dialog based on the detected emotions of target users, including emotional cues that no human could detect. These emotions could infer which conversational threads are eliciting a positive reaction and which are being met with resistance, allowing the AI to quickly adapt its tactics for optimised influence. This could make for a persuasive medium that exceeds any prior form of advertising.

STANDARDS OR REGULATION:
Consumers should have **the right not to be emotionally assessed** by software systems at speeds and using trait detection that exceed natural human abilities. This means **not allowing vital signs and micro-expressions** to be used in emotion detection [3, 5, 12].

STANDARDS OR REGULATION:
The risk to emotional privacy is amplified by the ability of platforms to collect emotional data over time and create profiles that allow AI systems to predict their reactions to a wide range of stimuli throughout their daily life. This could be the basis for highly predatory manipulation. Regulators should consider banning emotional profiling of all kinds, but especially for any use in the delivery of promotional content or influence campaigns [3, 5, 12].

STANDARDS OR REGULATION:
Without regulation, conversational agents could be designed to adjust their promotional tactics mid-dialog based on the detected emotions of target users. It could be so persuasive, in fact, it crosses the line from marketing to manipulation. For these reasons, use of **real-time emotional analysis for persuasive purposes should be banned or strictly regulated.** This is especially true when it involves detecting vital signs, micro expressions, subtle vocal traits and other subtle cues not normally perceived by humans in conversation [3, 5, 12].

3. The Right to Behavioural Privacy

CONTEXT: To successfully create the illusion that a user is immersed within a virtual or augmented world, extensive behavioural data needs to be tracked. Without that data, it could be impossible for platforms to simulate immersive experiences in real-time. This data includes very detailed information about where each user is located and what direction they're looking, as well as potentially including information about their gait, posture, eye-tracking, face-tracking, and vital signs.

That said, such data is only needed at the moment these experiences are being simulated. There is no inherent need to store this personal data over time. This is important because the storage of behavioural data can be used to create invasive personal profiles that document the daily actions of individual users in extreme detail. Such data could be processed by AI systems to predict how individual users will act, react, and interact in a wide range of circumstances during their daily life. And because metaverse platforms will have the ability to alter environments for persuasive purposes, profiles could be used to pre-emptively manipulate behaviours with accurate results.

STANDARDS OR REGULATION:
Policymakers should consider **banning metaverse platforms from storing behavioural data over time**, thereby preventing platforms from generating detailed profiles (and AI models) about their users that can predict their actions over time. In addition, **metaverse platforms should be restricted in correlating emotional data** with behavioural data, for such correlations could allow for promotionally altered experiences that don't just guide what users do in immersive worlds, but predictively influence how they're likely to feel while doing it [3, 5, 12].

4. The Right to Human Agency

CONTEXT:
Unless regulated, Metaverse platforms will have the ability extensively track the behaviours and emotions of users in real-time and profile users over long periods, creating AI models that predict their actions and reactions. In addition, unregulated metaverse platforms will be able inject targeted promotional experiences into the immersive environments of users, guiding their behaviours, emotions, or beliefs. The ability to track and impart influence in real-time, optimised by AI technologies creates a very dangerous problem wherein "real-time feedback loops" can be used to gradually optimise influence on individual users. This is known as the **"AI Manipulation Problem"** [31, 32, 37] and it refers to scenarios in which an AI-powered system: (i) imparts targeted influence on an individual user, (ii) senses the user's reaction to that influence, and (iii) repeatedly adjusts the influence tactics while sensing the user's real-time reactions to gradually maximise the persuasive impact. This might sound like an abstract process, but we humans usually just call it — a conversation. And we can expect AI powered avatars to pursue these feedback-control tactics in the near term unless strictly regulated [37].

STANDARDS OR REGULATION:
As described above, Metaverse platforms could easily deploy feedback-control systems that impart influence and monitor user reactions in real-time, thereby optimising their persuasive impact. This could greatly impact the cognitive liberty and epistemic agency of targeted users. Policymakers should consider aggressive and meaningful regulations that protect populations from manipulation by banning or highly restricting any system that "closes the loop" around users in real-time and establishes AI-powered feedback control systems that imparts persuasion, coercion or manipulation.

The functionality of technology that is used to target and manipulate people in the Metaverse is largely AI driven. As such, this focus on potential Standards to prevent targeted influence and manipulation in the Metaverse also supports the Federal Minister for Industry and Science, Ed Husic's statement that Australia should aim to be the leading country in Responsible AI, globally.

The role of Standards Australia

There is a current opportunity for Standards Australia, Australia's premiere standards organisation, to become a world leader in setting standards for the Metaverse, as outlined in this paper.

It is recommended that Standards Australia select a focus area for Standards for the Metaverse, such as **Standards to prevent targeted influence and manipulation in the Metaverse,** that builds on the existing work in online safety and Safety by Design and potentially include a lens that has an additional focus on children.

Suggested next steps to develop this focus area for Standards Australia include:

1. Presenting and promoting the Metaverse Standards Whitepaper and gathering feedback on its content and recommendations
2. Convening a panel of experts to determine the scope of work for the establishment of Metaverse Standards with a focus on *'Targeted influence and manipulation in the Metaverse'*
3. Conducting a thorough review of other related work that exists with other international Standards bodies, governments regulators, policy makers, academics and private sector organisations
4. Securing funding to research and create the Standards
5. Conduct consultation with industry, government and other relevant parties
6. Prepare comprehensive *Targeted influence and manipulation in the Metaverse* Standards documentation
7. Promote these Standards internationally

The need for Standards

> *"When you invent new technology you uncover a new class of responsibilities"*
> —Tristan Harris

> *"Without standards, there can be no improvement"*
> —Taiichi Ohno.

As noted in this paper there are few existing Standards for the Metaverse. Venture Beats comments that "The truth is that currently a lot of those standards and standardised approaches are missing and still need to be created. A simple example of this can be found around mapping and the simultaneous localisation that will be essential to create the mix of physical and digital augmented realities that could make up the metaverse. Today, device manufacturers and platforms each have their own proprietary data for this process, and there is nothing that could pass for an agreed standard."

Due to the evolving nature of the Metaverse, it may take some time before laws and regulations come into full effect. In the meantime, standards can provide the Metaverse stakeholder a baseline for mutual understanding as well as tools to create, connect, measure results, communicate, and do commerce. This makes standards an essential tool to "fill the gap", to define good practices, and to enable innovation.

Metaverse risks such as human, societal, information, legal and regulatory, information and financial risks need to be addressed in a holistic manner and it can only be achieved through standards and frameworks. For example, if accessibility standards are not established, people with disabilities could remain excluded from accessing and benefiting from the Metaverse.

> *"The social consequences of a technology cannot be predicted early in the life of the technology. When change is easy, the need for it cannot be foreseen; when the need for change is apparent, change has become expensive, difficult and time-consuming."*
>
> —David Collingridge

With the evolution of the Metaverse we are presented with the "Collingridge Dilemma" leads us into the following double-bind problem when it comes to risks related to the Metaverse:

1. **An information problem:** impacts cannot be easily predicted until the Metaverse is extensively developed and widely used.
2. **A power problem:** control or change is difficult once the Metaverse has become fully entrenched.

Hence, the standards and frameworks are required to prevent harm before it is too late. The Collingridge dilemma equally applies to data collection in the Metaverse. Data is the heartbeat of the Metaverse. Meaningful experiences can only be realised when we use contextual data about an individual for that individual's experience. This inherently means developers need to know information about people – where they are, what they're looking at, if they're moving or not, etc. Developers may likely opt for a "more is better" approach when it comes to data collection. This is where standards and frameworks such as data minimization, Privacy Enhancing Techniques (PETs), Privacy by Design, Safety by Design, etc could prevent privacy, safety and security harms in the Metaverse.

The risks of not having Standards for the Metaverse include four major categories:

Risk to Individuals

Individuals will experience some level of impact from the adoption of the Metaverse globally. The risks could be exacerbated for the vulnerable population such as civil liberties, elderly, children, people with disabilities, etc. The Metaverse could expose individuals to harassment, abuse, manipulation, bullying, discrimination, addiction, mental health issues, privacy, human rights, autonomy etc.

Risk to Societies
The Metaverse will create social inequalities, digital divides and cultural clashes among different groups of individuals. Misinformation, disinformation, and propaganda could be amplified, potentially undermining social norms, values and social constructs such as Democracy. The loss of privacy at the societal level itself could have serious consequences, like economic uncertainty.

Risk to Governments
The very nature of the Metaverse, i.e., convergence of several different technologies including Artificial Intelligence could potentially undermine government authorities. It could also pose threats to national security, public order and democracy by facilitating crime, terrorism and misinformation. The Metaverse will challenge the authority and jurisdiction around the ownership, governance, and policing. The lack of governmental engagement could create economic inequalities if not addressed proactively.

Risk to Ecosystems
The Metaverse will cause a variety of risks to industries, organisations and in general the ecosystems. These risks could negatively impact organisations' business operations, security, and reputation stemming from data breaches, privacy issues, identity management issues, and cyberattacks. These risks could expand to the interdependent and interconnected elements within the Metaverse, such as virtual currencies, social networks, and immersive experiences. The global financial systems, supply chain or interrelated systems that depend on the metaverse for transactions and communication, could also be impacted. Depending on the energy consumption and greenhouse emissions from the metaverse infrastructure could pose risks to the natural resources, environment and our planet.

In sum, we need to learn from the lessons of Web2.0 and social media where we did not get ahead of the technology and anticipate risks and write Standards for them, and now we have the chance, as Australians, to be leading advocates for a safe and responsible Metaverse through the work of Standards Australia and setting guidelines for the manipulation of people in the Metaverse.

Additional topics for Standards for the Metaverse

In addition to the recommended focus area of Standards for targeted influence and manipulation in the Metaverse the following could be considerations for Standards Australia to work on the following three areas:

1. Extending Safety by Design to include Metaverse standards
2. Focusing on Responsible AI aspects of Metaverse platforms and extending the Responsible AI frameworks to these
3. Child Safety Standards

Concluding remarks

For the Authors of this report, there is no doubt that the Metaverse is real and is being developed at a rapid rate. So that the significant challenges of Web2.0 and social media are not repeated at scale in a completely immersive environment – it is essential that we get develop Standards which can then be used to inform policy, regulation and legislation.

A thorough review of work that is been done on Standards internationally, plus analysing the areas that Australia already excels at with regard to Standards, policy and regulation, then the strong recommendation for Standards Australia is to focus on the development of Standards that relate to targeted influence and manipulation in the metaverse.

If this is done, then Australia can take a lead role in the creation of a safe and responsible Metaverse.

Citations

1. Zuckerberg, Mark (2021) Founder's letter, 2021, Letter to Shareholders 2021. Meta. Available at: https://about.fb.com/news/2021/10/founders-letter/
2. Stephenson, Neal (1993). Snow Crash. New York, Bantam Books.
3. Rosenberg, Louis. "Regulation of the Metaverse: A Roadmap: The risks and regulatory solutions for large scale consumer platforms." In Proceedings of the 6th International Conference on Virtual and Augmented Reality Simulations, pp. 21-26. 2022.
4. Rosenberg, Louis (2022). Augmented Reality: Reflections at Thirty Years. In: Arai, K. (eds) Proceedings of the Future Technologies Conference (FTC) 2021, Volume 1. FTC 2021. Lecture Notes in Networks and Systems, vol 358. Springer, Cham. https://doi.org/10.1007/978-3-030-89906-6_1
5. Rosenberg, Louis (2022). Regulating the Metaverse, a Blueprint for the Future. In: De Paolis, L.T., Arpaia, P., Sacco, M. (eds) Extended Reality. XR Salento 2022. Lecture Notes in Computer Science, vol 13445. Springer, Cham. https://doi.org/10.1007/978-3-031-15546-8_23
6. Hatami, H. et al. (2023) A CEO's guide to the Metaverse, McKinsey & Company. McKinsey & Company. Available at: https://www.mckinsey.com/capabilities/growth-marketing-and-sales/our-insights/a-ceos-guide-to-the-Metaverse
7. Person (2022) Company documents show Meta's flagship Metaverse falling short, The Wall Street Journal. Dow Jones & Company. Available at: https://www.wsj.com/articles/meta-Metaverse-horizon-worlds-zuckerberg-facebook-internal-documents-11665778961
8. Cohen, A. (2022) Metaverse platforms Decentraland, the sandbox see less than 1,000 daily active users, according to data from DappRadar, Decentraland, The Sandbox See Less Than 1,000 Daily Active Users. Sports Business Journal. Available at: https://www.sportsbusinessjournal.com/Daily/Issues/2022/10/10/Technology/Metaverse-decentraland-the-sandbox-daily-active-users (Accessed: March 12, 2023).
9. Bradshaw, T. and McGee, P. (2023) Tim Cook bets on Apple's mixed-reality headset to secure his legacy, Subscribe to read | Financial Times. Financial Times. Available at: https://www.ft.com/content/86b99549-0648-4c23-ab6e-642a4ba51dff (Accessed: March 12, 2023).
10. Pearlman, Kavya (2018) Virtual Worlds - Real Risks, Cybersecurity Quarterly (Fall 2018). Available at: https://issuu.com/cybersecurityquarterly/docs/csq_volume_2_issue_3 (Page 15-16).
11. Breves, Priska (2021). "Biased by Being There: The Persuasive Impact of Spatia lPresence on Cognitive Processing." Computers in Human Behavior, vol.119, 2021, p. 106723., https://doi.org/10.1016/j.chb.2021.106723
12. Rosenberg, Louis (2022), "Marketing in the Metaverse and the Need for Consumer Protections," 2022 IEEE 13th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, NY, USA, 2022, pp. 0035-0039, https://doi.org/10.1109/UEMCON54665.2022.9965661
13. Atske, S. (2021) 1. personal experiences with online harassment, Pew Research Center: Internet, Science & Tech. Pew Research Center. Available at: https://www.pewresearch.org/internet/2021/01/13/personal-experiences-with-online-harassment/
14. Atske, S. (2022) Teens and cyberbullying 2022, Pew Research Center: Internet, Science & Tech. Pew Research Center. Available at: https://www.pewresearch.org/internet/2022/12/15/teens-and-cyberbullying-2022/
15. Lawson, Eli Cohen. "New Research Shows Metaverse Is Not Safe for Kids - Center for Countering Digital Hate: CCDH." Center for Countering Digital Hate | CCDH, May 17, 2022. https://counterhate.com/blog/new-research-shows-Metaverse-is-not-safe-for-kids/.
16. Nightingale, S., Hany, J.F.: AI-synthesized faces are indistinguishable from real faces and more trustworthy. In: Proceedings of the National Academy of Sciences (2022). https://doi.org/10.1073/pnas.2120481119
17. Rosenberg, L. (2023). Marketing in the Metaverse: Emerging Risks. In: Arai, K. (eds) Advances in Information and Communication. FICC 2023. Lecture Notes in Networks and Systems, vol 651. Springer, Cham. https://doi.org/10.1007/978-3-031-28076-4_5
18. Bell, C. (2022) The Metaverse is coming. here are the cornerstones for securing it., Official Microsoft Blog: https://blogs.microsoft.com/blog/2022/03/28/the-Metaverse-is-coming-here-are-the-cornerstones-for-securing-it/
19. Rosenberg, Louis (2022). "Evil Twins and Digital Elves: How the Metaverse Will Create New Forms of Fraud and Deception." Big Think, April 22, 2022. https://bigthink.com/the-future/Metaverse-fraud-digital-twins/
20. Verma, Pranshu. "They Thought Loved Ones Were Calling for Help. It Was an AI Scam." The Washington Post. WP Company, March 10, 2023. https://www.washingtonpost.com/technology/2023/03/05/ai-voice-scam/.
21. Commission on Information Disorder Final Report, Aspen Institute (2021). https://www.aspeninstitute.org/publications/commission-on-information-disorder-final-report/AspenDigital
22. Rosenberg, Louis. (2023). The Growing Need for Metaverse Regulation. In: Arai, K. (eds) Intelligent Systems and Applications. IntelliSys 2022. Lecture Notes in Networks and Systems, vol 544. Springer, Cham. https://doi.org/10.1007/978-3-031-16075-2_39
23. Ivanova, E.,Borzunov, G.: Optimization of machine learning algorithm of emotion recognition in terms of human facial expressions. Procedia Computer Science 169, 244–248 (2020)
24. van den Broek, E.L., Lisý, V., Janssen, J.H., Westerink, J.H.D.M., Schut, M.H., Tuinenbreijer, K.: Affective man-machine interface: unveiling human emotions through biosignals. In: Fred, A., Filipe, J., Gamboa, H. (eds.) BIOSTEC 2009. CCIS, vol. 52, pp. 21–47. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-11721-3_2
25. Boz, H., Kose, U.: Emotion extraction from facial expressions by using artificial intelligence techniques. BRAIN .BroadRes. ArtificialIntell. Neuroscience 9(1) ,5–16 (2018). ISSN2067– 3957
26. Zarouali, B., et al.: Using a personality-profiling algorithm to investigate political microtargeting: assessing the persuasion effects of personality-tailored ads on social media. Communication Res. 0093650220961965 (2020)
27. Van Reijmersdal, E.A., et al. Processes and effects of targeted online advertising among children. Int. J. Advertising 36(3), 396–414 (2017)

28. Rosenberg, Louis (2021). “Metaverse: Augmented Reality Pioneer Warns It Could Be Far Worse than Social Media.” Big Think. Freethink Media, November 6, 2021. https://bigthink.com/the-future/Metaverse-augmented-reality-danger/
29. Hirsh, J.B., Kang, S.K., Bodenhausen, G.V.: Personalized persuasion: tailoring persuasive appeals to recipients’ personality traits. Psychol. Sci. 23(6), 578–581 (2012)
30. Wojdynski, B.W., Evans, N.J.: The covert advertising recognition and effects (CARE) model:
31. Rosenberg, Louis (2023) “The Metaverse and Conversational AI as a Threat Vector for Targeted Influence,” in Proc. IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC), 2023. https://www.researchgate.net/publication/368492998_The_Metaverse_and_Conversational_AI_as_a_Threat_Vector_for_Targeted_Influence
32. Rosenberg, Louis (2023). “Conversational AI Will Learn to Push Your Buttons.” Barron’s. February 23, 2023 https://www.barrons.com/articles/conversational-ai-will-learn-to-push-your-buttons-manipulation-problem-c9f797e8
33. “Addictive Behaviours: Gaming Disorder.” World Health Organization. World Health Organization. https://www.who.int/news-room/questions-and-answers/item/addictive-behaviours-gaming-disorder.
34. Skarredghost. “VR Is 44% More Addictive than Flat Gaming (According to a Study).” The Ghost Howls, March 2, 2022. https://skarredghost.com/2022/03/02/vr-virtual-reality-Metaverse-addictive/
35. A. V. Rajan et al., “Virtual Reality Gaming Addiction,” 2018 Fifth HCT Information Technology Trends (ITT), Dubai, United Arab Emirates, 2018, pp. 358-363, doi: 10.1109/CTIT.2018.8649547
36. Ryan-Mosley, T. (2021) Beauty filters are changing the way young girls see themselves, MIT Technology Review. MIT Technology Review. https://www.technologyreview.com/2021/04/02/1021635/beauty-filters-young-girls-augmented-reality-social-media/

Resources

- XRSI definitions https://xrsi.org/definition/the-metaverse
- Metaverse governance https://www.academia.edu/66984560/Securing_the_Metaverse_Virtual_Worlds_Need_REAL_Governance
- Capterra Research - https://www.capterra.com.au/blog/3282/research-study-is-metaverse-the-future-australia
- Core enablers of the metaverse - https://www.matthewball.vc/all/forwardtothemetaverseprimer
- Technology Magazine - https://technologymagazine.com/articles/top-10-best-metaverse-platforms-to-look-out-for-in-2023
- Cryptovoxels https://www.voxels.com/
- Unity Technologies https://unity.com/
- The Sandbox https://www.sandbox.game/en/
- Roblox https://www.roblox.com/
- Decentraland https://decentraland.org/
- Epic Games https://www.epicgames.com/site/en-US/home
- NVIDIA Omniverse https://www.nvidia.com/en-au/omniverse/
- Microsoft Mesh https://www.microsoft.com/en-us/mesh
- Meta Horizons World https://www.meta.com/au/horizon-worlds/
- Niantic https://nianticlabs.com
- Bytedance PICO https://www.engadget.com/pico-4-vr-headset-bytedance-150028514.html
- Start US Insights https://www.startus-insights.com/innovators-guide/metaverse-startups/
- XRSI standards https://xrsi.org/research-standards
- Pew Research https://www.pewresearch.org/internet/2021/01/13/the-state-of-online-harassment/
- Khronos Group https://www.khronos.org/
- Metaverse Standards Forum https://metaverse-standards.org/
- OMG https://omigroup.org/
- W3C https://www.w3.org/
- Virtual World Society https://www.virtualworldsociety.org/
- Computer Technology Association https://www.cta.tech/
- IEEE https://www.ieee.org/
- International Telecommunication Union https://www.itu.int/en/Pages/default.aspx
- Open Geospatial Consortium https://www.ogc.org/
- World Economic Forum https://www.weforum.org/
- Online Safety Act https://www.legislation.gov.au/Details/C2021A00076
- Enhancing Online Safety for Children Act of 2015. https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/105255/128681/F249839433/AUS105255%202017.pdf
- eSafety Commission https://www.esafety.gov.au/
- Safety by Design https://www.esafety.gov.au/industry/safety-by-design
- Immersive Technology Challenges https://www.esafety.gov.au/industry/tech-trends-and-challenges/immersive-tech
- Token Mapping https://treasury.gov.au/consultation/c2023-341659
- Australian Artificial Intelligence Ethics Framework https://www.industry.gov.au/publications/australias-artificial-intelligence-ethics-framework
- Research on Australian online internet penetration rates https://datareportal.com/reports/digital-2022-australia#:~:text=Internet%20use%20in%20Australia%20in%202022&text=Australia’s%20internet%20penetration%20rate%20stood,percent)%20between%202021%20and%202022
- Venture Beats https://venturebeat.com/datadecisionmakers/without-standards-there-is-no-metaverse/
- Collingridge Dilemma https://en.wikipedia.org/wiki/Collingridge_dilemma

Appendix

Top 10 Metaverse platforms as noted by Technology Magazine, 26 January 2023 -

Cryptovoxels

Cryptovoxels is a virtual world platform that allows users to buy, sell, and own virtual land using cryptocurrency. It is built on the Ethereum blockchain and has a growing community of creators and developers. The virtual world is made up of a grid of parcels, each one of which can be purchased and owned by an individual or organisation. Users can then use these parcels to build and create their own virtual experiences, such as games, art installations, and social spaces.

Unity Technologies

Through Unity Technologies' platform, developers can also use the Unity Engine to develop metaverse experiences. In November 2021, Unity acquired the digital VFX company Weta Digital in a deal exceeding $1.6bn. Through this acquisition, and Weta's focus on VFX tools, Unity is hoping to accelerate its development of real-time 3D technologies, and their deployment in the metaverse.

The Sandbox

The Sandbox is a metaverse platform that allows users to create and monetise their own virtual worlds and experiences using NFTs on the Ethereum blockchain. Users can buy, sell, and trade virtual real estate and assets in a secure and transparent way, without the need for a central authority. The Sandbox also offers a creative suite of tools to make it easy for users to create and customise their own virtual worlds, experiences, and games. It also has a strong community of creators and developers who are building and experimenting with new ways to use the platform, and a strong partnership with major players in the gaming and entertainment industry such as Atari, Binance, and Square Enix.

Roblox

Roblox is a global online gaming platform, which also pioneers the development of metaverse gaming experiences. Through Roblox, users can create and share their own games and experiences, program games themselves, and play games that have been developed by other users.

The platform was created by Roblox Corporation in 2006 and is available on a variety of platforms, including PC, mobile, and gaming consoles. It has a large and active user base, with over 150 million monthly active users, and has become a major player in the gaming industry.

Decentraland

Decentraland is a virtual reality platform that utilises blockchain technology to create a decentralised and immersive online world. The platform allows users to create and monetize their own content, as well as buy and sell virtual real estate and assets as NFTs via the MANA cryptocurrency.

Opened to the public in February 2020, Decentraland uses the Ethereum blockchain, which allows for secure and transparent transactions within the virtual world. This means that users can be sure that their virtual assets and land are truly theirs and can be bought and sold without the need for a central authority.

Google Starline

Aiming to enable real-time, 3D communication between people in different locations, Google Starline uses a combination of computer vision, machine learning, and spatial audio to create a shared, immersive experience that makes it feel like people are in the same room together.

The technology is based on a combination of cameras, microphones, and displays, and is designed to be used in a specialised booth that is equipped with these components. Google Starline is still in the research and development stage and is not yet available for commercial use. The company has not announced a release date, or any further details about the technology's availability or pricing.

Epic Games

Epic Games is a video game developer and publisher that is known for creating popular titles such as Fortnite and Unreal Engine. The company has recently announced plans to enter the metaverse space and to develop a social and gaming platform that will connect players across different games and virtual worlds.

Epic Games plans to leverage its expertise in game development, its large player base, and its successful business model, to create a metaverse platform that will allow users to interact, socialise, and play games in a shared virtual space. The company is also developing new technology, such as the MetaHuman Creator, a tool that allows users to create highly realistic and customizable human avatars, to enhance the metaverse experience.

NVIDIA Omniverse

NVIDIA Omniverse is a virtual reality and simulation platform developed by NVIDIA, a leading technology company in the field of computer graphics and AI. Omniverse is designed to bring together various industries such as film, gaming, product design, and architecture, by providing a collaborative and immersive environment for users to create and simulate their projects. The platform utilises the power of NVIDIA's hardware and software technologies, such as ray tracing and AI, to provide a realistic and high-quality visual experience.

NVIDIA Omniverse also offers a wide range of tools and features to make it easy for users to create and customise their own virtual worlds and experiences. It also has a growing community of developers and creators who are building and experimenting with new ways to use the platform.

Microsoft Mesh

Microsoft Mesh is a platform developed by Microsoft that enables users to connect and collaborate in mixed reality across devices and locations. The platform allows users to create, and experience shared virtual and augmented reality environments, enabling them to interact with each other and with digital content in a more natural and intuitive way.

One of the key features of Microsoft Mesh is its ability to connect multiple devices and platforms, such as virtual and augmented reality headsets, smartphones, and PCs, allowing users to collaborate and share their experiences across different devices and locations. This allows users to work on a project together, regardless of their location, and can also help to reduce development time and costs.

Meta Horizon Worlds

One of the global leaders in metaverse investments, Meta is renowned across the world for being one of the biggest advocates of the metaverse's role in future industries and social applications.

Its Horizon Worlds virtual platform aims to create a decentralized and immersive online experience for users. The platform utilises blockchain technology to create a secure and transparent virtual world where users can own, buy and sell virtual assets and real estate, and interact with others in a shared virtual space. It is built on the Ethereum blockchain and has a growing community of creators and developers.

The platform also has a growing community of developers and creators, who are building and experimenting with new ways to use the platform. Meta Horizon Worlds also has a strong focus on user-generated content and encourages users to create and share their own experiences.

Metaverse Start Ups

RLTY delivers 3D Immersive Experiences

RLTY is a metaverse startup that builds a no-code startup platform to build 3D immersive experiences for the metaverse. It combines virtual reality (VR), cloud computing, blockchain, and a game engine to organize concerts, festivals, art exhibitions, and more. The platform also allows collaborators to manage access-control list (ACL) rights and easily onboard 3D artists to optimize events. This event management workflow enables event organizers and entertainment companies to mitigate coding and in-house software development. Consequently, they are able to build and launch web3 and metaverse events faster as well as improve customer or end-user experience.

Kirin Metaverse maintains a Web3 Social & Gaming Infrastructure

Kirin Metaverse is a US-based startup that offers a web3 social and gaming Infrastructure. The startup's no-code creator studio leverages generative AI and proprietary pre-training techniques to produce interoperable avatars and assets. The assets are rendered as GLB models that are minted and used in the metaverse. The studio's machine learning (ML) model also handles weapons, chests, and even environmental assets like trees and doors. This allows metaverse users to create customized avatars while enabling game studios to automate otherwise time-consuming in-game assets and avatar development.

Bit.Country offers Metaverse as a Service

Bit.Country is a Singaporean startup that provides metaverse as a service. The startup's metaverse network, Metaverse.Network, allows non-technical users to launch their metaverse projects. Bit.Country's application programming interface (API) also enables them to develop games and smart contract decentralized apps (dApps). The startup's metaverse includes a non-fungible token (NFT) marketplace, map engine, land economy, NFT facilities, and a customizable 3D world engine. Further, Metaverse.Network allows project owners to incentivize users that contribute to the community and supports the integration of existing decentralized applications (dApps). This allows them to accelerate project development and reach a wider audience.

Edverse builds an Educational Metaverse

Edverse is an Indian startup that makes an educational metaverse. The startup utilizes Polygon and Elysium blockchains to create a public decentralized network and deliver education history as NFT records. It also offers a metaverse space to host virtual classrooms and alumni meetups as well as conduct joint classes. The startup's 3D library of educational assets, Ed-NFT 3D Library, offers numerous educational assets to educators and learners. Further, the metaverse's tokenomics incentivizes the stakeholders to earn EDV tokens for opting into various courses. This allows schools to reach a wider student pool and improve their educational model.

landindex provides Metaverse Data Analytics

Metaverse startup **landindex** develops a metaverse data analytics tool. It aggregates metaverse data from Decentraland, The Sandbox, NFT World, Otherside, and other virtual worlds. The tool then provides an overview of land price, ownership, and investment across these virtual spaces. Moreover, the startup's API delivers updates on the land value through live NFT prices without depending on third parties like OpenSea. This price index and analysis tool thus allow investors and users to track metaverse activities and identify high-performing spots in the metaverse.

Veyond Metaverse builds a Healthcare Metaverse Ecosystem

Veyond Metaverse is a US-based startup that maintains a healthcare metaverse ecosystem. The startup's proprietary cloud communication platform leverages extended reality (XR), AR, and VR to improve collaboration and engagement. It enables surgeons to create, manipulate, and interact with patient digital twins. This enables remote surgical training, remote supervision of surgeries, and real-time collaboration between surgeons. The platform also supports various haptic devices and features AI to offer an immersive metaverse hospital. As a result, Veyond

Metaverse allows clinicians to collaborate in real time and enables simultaneous surgical education, training, planning, and collaborative procedures.

Metaboutiq makes Wear-to-Earn NFTs

Estonian startup **Metaboutiq** creates wear-to-earn NFTs. The startup's marketplace provides limited collections of curated 3D outfits for use in virtual work and leisure spaces. Metaboutiq also partners with social media influencers to promote NFTs. The startup's NFTs are interoperable across AR and VR ecosystems, allowing users to deploy custom outfits in numerous metaverse networks.

Next Earth offers Metaverse Land Ownership

Next Earth is a Hungarian startup that develops a metaverse land ownership platform. It allows users to own locations on earth as NFT lands and connect them to their web2 business websites or platforms. The startup's platform also allows developers to build map-based applications using smart contracts and minting dynamic NFTs. This allows owners to buy and sell Next Earth's lands on their terms and enables them to earn money by staking their NFTs for activities in their virtual land. Further, the startup's platform as a service solution provides the resources, infrastructure, and user base required for businesses to expand or transition into the metaverse. This greatly cuts down in-house development costs and project launch time.

Black History DAO delivers Immutable Black History Records

Black History DAO is a US-based decentralized autonomous organization (DAO) that makes immutable black history records. The startup collects, preserves, and shares real stories of Black history and anchors them on the blockchain. For this, it utilizes peer-reviewed submissions and rewards contributors with BHD tokens. Further, Black History DAO delivers this data in the metaverse through AR and VR to make the data more accessible and discoverable. The startup also donates a part of its wealth to preserve historical landmark sites.

KEYS Metaverse builds an Open Metaverse

KEYS Metaverse is a UAE-based startup that makes an open metaverse that focuses on accessibility and immersive user experiences. The startup's device-agnostic metaverse is built on Unreal Engine 5 and is accessible through a **URL**. It allows users to access the metaverse more flexibly and supports all devices that feature bi-directional streaming. The real estate-centric metaverse also offers a 3D marketplace to engage global real estate buyers and sellers. KEYS Metaverse further provides creator tools and professional services that allow community members to build custom businesses and utilities in its metaverse.

standards.org.au