Metaverse Policy Think Tank

Introduction

On 5th October 2022 the Responsible Metaverse Alliance hosted its first **Metaverse Policy Think Tank.**

The aim of the Metaverse Policy Think Tank was to identify opportunities to collaborate with policy stakeholders on Responsible Metaverse initiatives and validate the interest of attendees to participate in a global metaverse policy forum.

Attendees at the Metaverse Policy Think Tank included an Australian government State Minister, Federal and State Commissioners, government officials, policy makers and regulators across Australia and New Zealand as well as responsible metaverse activists from the UK and the US (please see list of attendee organisations in the appendix).

Summary points

- The metaverse is a persistent and immersive virtual or augmented world that is experienced in the first person by large groups of simultaneous users who share a strong sense of mutual presence.

- The metaverse provides highly immersive experiences for people, however it is currently ungoverned, and the risks posed are expected to be substantially more significant compared to Web 2.0 and social media.

- Key risk drivers include dangers from: other users, bad actors and corporations (such as big tech). Risks of the metaverse include but are not limited to identity fraud, harassment and abuse, sex related harms, financial risks, scams, intellectual property risks, contract risks, data privacy and control risks, national security, human trafficking, organised crime, and terrorism threats.

- Powerful tech companies who already have a large amount of data from individuals, organisations, governments, and other entities will have vastly more data and will be able to potentially coerce or manipulate people in an unprecedented way. The metaverse may blur boundaries of what is real and not real. Persuasion, advertising, and propaganda will potentially be designed into immersive experiences used for promotional purposes.

- The time to design and develop metaverse regulation and policy is now, ahead of the projected 3 to 5-year period when the metaverse may have mainstream usage.

- Potential areas for policy and regulation to address:

    1. Protection of children
    2. Protection of the vulnerable
    3. Accessibility
    4. Identity in the metaverse
    5. Safety by Design requirements being extended to the metaverse
    6. Ethical by Design requirements being extended to the metaverse
    7. Applying existing human rights policies to the metaverse
    8. Intellectual property protection
    9. The use and transparency of Virtual Avatars or Spokespeople and Virtual Products
    10. Law enforcement, policing and Crime Stoppers
    11. National Security

    More specific recommendations for policy may include:

    1) Prohibit Behavioural Profiling in the metaverse
    2) Prohibit Emotional Profiling in the metaverse
    3) Require all promotional content (especially targeted content) to be clearly identifiable as promotional material
    4) Ban immersive advertising for children
    5) Prohibit the use of real-time biometric or emotional data in any form of interactive content other than for approved health and wellness applications (ideally certified)
    6) Monitor extremist groups organising or re-organising in the metaverse

Key Discussion Points

Key topics of discussion are set out below.

Discussion #1 - Introductory statements

The session commenced with leaders offering introductory statements. Key points from these statements included:

- The Responsible Metaverse Alliance's working definition of a Responsible Metaverse is:

    A Responsible Metaverse is one where immersive worlds have been designed, developed, deployed and operate in a manner which has the well-being of the diverse participants, civil society and the environment at its core; and that platform providers and related parties are held to account for any harm that might be caused.

- There is a need to urgently act on establishing regulation for the metaverse so that the mistakes of Web2.0 are not repeated and so that new risks associated with the metaverse are identified and mitigated.

- Governments need to be inclusive in how they deliver services in the metaverse, given that in the future most of the service delivery will be through digital channels e.g the digital drivers licence that the NSW government has issued.

- As we start to move into this area, we need to ask - is the metaverse a safe environment? - given there are many examples of Web 2.0 in application with highly detrimental outcomes.

- As we move into Web3 we must have more control and put trust mechanisms and a responsible framework in place and scan the globe for best practice.

- The NSW Government will be communicating its Metaverse Strategy, supported by the Gradient Institute, in November 2022.

- There are a myriad of ways humans can exploit technology, inflict personal harms and create reputational, revenue or regulation risks or threats.

- For the metaverse the concept of Safety by Design should not be revolutionary. Cars are safer on the road with seat belts; there is now a focus on safe food. Architects of new digital constructs need their own seatbelt moment.

- All VR and MR blur the lines of what's real or not but create new immersive experiences – so we'll likely see escalation of bullying, hate, abuse and harassment. These experiences are more traumatic in immersive environments than it is in today's Web 2 world.

- The metaverse is currently developing with no guardrails. Research into safety in the metaverse notes that 1 in 5 Australians said they experienced something that made them feel unsafe, 80% feel tech and gaming companies should be the ones responsible to keep people safe.

- Australia has a 7-year runway regulating online harms. As threats continue to evolve the policy landscape has to evolve with it, if not ahead of it, without stifling innovation.

- We need to assess risks and benefits of new tech and not overregulate.

- In the first instance we just need to hold companies' feet to fire. So, they place the safety of people first.

- We've seen the development of safe zones in the metaverse however the tools for the web 2 world are not sufficient for the metaverse eg blocking tools. Harm will happen in real time. We need an eject button. We need to think about it now. We need legal notices to lift the hood on what major platforms are doing. We need to look at this on a number of fronts:

1. Prevention - through education
2. Prevention through incentives
3. Protection through investigation or removal schemes
4. Continuing proactive systemic change

- Everybody should be able to participate online in a way that keeps them safe, protects culture and meets the obligations of partners of treaty.

- A focus should be on the positive and negative impacts on culture and art; how CSAM (Child Sexual Abuse Material) manifests in the metaverse, specifically with haptic tech coming; how violence and extremism will manifest; how training will be conducted of extremist groups; how attacks may occur; how harms will be monetized; and how the metaverse makes an experiential space for the perpetrator and victim.

- Current legislative frameworks are not equipped for the metaverse. The focus to date has been educating people on opportunities and risks. When people think about the metaverse it feels 10-20 years away and not something that's here today.

- In New Zealand, education has been focused on a metaverse 101 presentation to 600 public servants. The New Zealand government is now extending this presentation to pacific partners and hopes that Safety by Design will feature in the metaverse.

- Web 1 was created by idealists and the web had unprecedented potential; web 2 saw much harm, marginalised groups, centralised structure and societal harms. In web 3 we have the opportunity to create the kind of reality we want to see. Pre-emptive actions towards privacy and security standards are needed.

- We are not only experiencing convergence of emerging technologies, but citizens around the world are uninformed about how they should prepare. Based on past 3-4 years of research we need to break down silos, focus on children with a Child Safety Framework, and shift responsibility to the platform companies, so that they do not just code for addictive engagement.

Discussion # 2 - Current work in the responsible metaverse field

- The attendees discussed relevant work that was being conducted currently.

- It was noted that the need for metaverse regulation crosses over a lot of the work that Human Rights Commissions are doing – such as the Children's Commissioner and Disability Commissioner.

- The metaverse has so much impact in terms of the harm for human rights, as well as the benefits. If we do this right, it could have so much benefit in terms of accessibility etc. There is an enormous urgency in taking this on, the biggest hurdle is the lack of understanding about the metaverse. We need to raise the issue with the people who are thinking through the policy considerations.

- Police senior executives need to become educated on the metaverse. The police are thinking about how they police, what laws are impacted, and the practicalities of people reporting a crime - e.g., someone being harassed or sexually assaulted. If this happened right now a police officer would not necessarily have a process to follow. There needs to be some consistency in their approach to policing in the metaverse. If something happens in the metaverse, then where did it happen? At the moment if a crime happens in New South Wales, then we might send it off to different jurisdictions. Then how would we address this with metaverse?

- Reference was made to the sense of moving ‘onward into the fog’ - into the unknown. Crime Stoppers is a federated model and to address the risks of the metaverse, we will need to bring together a cross-jurisdiction group. As Crime Stoppers is worldwide there might be an opportunity to bring people together that others can't.

- A discussion was had about Intellectual Property Rights in the metaverse, noting that registered IP rights can assist in realising the benefits of the metaverse, but a question was raised as to how we can do this in a way which assists those people building it. No-one is doing this well in IP rights internationally. An international approach to IP rights is very important for consistency of assessment. There will be different forces at play in how registered IP rights are happening in the metaverse. This hasn’t even necessarily been done well in web 2.0.

- Around the world, governments provide approximately 14 key services to citizens digitally. What does that mean for the metaverse? Will there be a burgeoning number of interactions with citizens? Some considerations break down to 4 components:

    1. Look at fundamental human rights
    2. Look at the transaction between governments and citizens and what it means in terms of preservation of human rights
    3. Government to business - IP rights should be open / accessible to citizens
    4. Global inclusion - because metaverse tech is global we need to not alienate huge numbers of people and create social disruption. We need to bear this in mind as we think about any regulator model.

Discussion # 3 - Risks of the metaverse

A discussion on risk led by Dr Louis Rosenberg noted that there were three main categories:

1. Dangers from other users
    - Problem - hate, harassment, bullying, assault all become immersive in the metaverse.
    - Solution - potential platform moderation although this is harder than social media
2. Dangers from bad actors
    - Problems - fraudsters, hackers, con artists, identity theft, virtual impersonation.
    - Solution - platform security, identity verification is critical for trust

3. Dangers from Big Tech
    - Problems – the metaverse will give platforms unparalleled power and influence. We’re familiar with types of problems from other users, familiar with bad actors, fraudsters, dangers from big tech, but this is a level we haven't seen before, the problem there is the platforms will give them unparalleled power and influence.
    - Solution - the only solution is regulation, otherwise we’ll see problems like social media but far worse.

- The tech is not what is to be feared, it is the power the platforms will have over users – driven by the business model.

- Tracking and profiling mean large third parties can track who your friends are, where you are, what you buy in the metaverse; when a person is immersed in a virtual world or in real world that's augmented, it tracks who you’re with in real time, where you look, how long your gaze lingers. If you walk through store in metaverse, they'll know what window you’re looking in for how long, they’ll track your gait and use this to judge interest levels; they will understand your behaviour at a deep level; they will monitor facial expressions, vocal inflections, infer emotions in real time, monitor vital signs, heart rate, blood pressure, and pupil dilation. These things will be put into devices for health and meditation but if unregulated this information will be used for profiling purposes, promotional purposes, detailed things about your emotions.

- The metaverse will be able to track everything you say and do and experience and infer what you feel about everything. That’s a privacy concern. In the metaverse these platforms can influence more extensively than social media, targeting children with news feeds. The whole point of the metaverse is to blur boundaries of what's real not real. Persuasion, advertising and propaganda won't be flat ads, it will be an immersive experience and can change the world around us for its promotional purpose. This is a recipe for dangerous situations.

- Advertising propaganda in the metaverse won't be advertisements, it will be product placements or people injected into your day without you knowing, such as walking down the street and seeing a parked car that was actually a targeted promotional experience but looks just as real as everything else. It is paid content by a third party. This level of influence could be related to products or it could be political messaging.

- In the metaverse, third parties alter our world without our knowledge, and it is dangerous, such as Promotional Spokespeople - avatars who engage us in conversation. This is only 2-3 years away. These aviators could be indistinguishable from other people in the environment and a person/avatar might think they are talking to another person/avatar, however it will be a Virtual Avatar. Promotional programs and their goals are to influence a person through conversation. The Virtual Avatar will have access to my history, all the data that's been collected and it will use that in promotional conversation.

- If not regulated, metaverse platform providers will track emotions and adjust tactics to influence people. Potentially these Virtual Avatars will pitch better than any human salesperson, influence more skilfully and promote propaganda more than ever before. This needs to be regulated.

- The metaverse will transform society in the next 10 years. Advances in AI are rapid, and risks are similar to what we're seeing in social media but worse. Now's the time to think of metaverse regulation before platforms develop their business models. That's where we failed with social media – we didn't see dangers early enough. With the metaverse we're at a formative stage, we could get regulation that can guide industry in other ways of competing, instead of competing on who can track or influence people.

Dr Rosenberg also shared slides which noted:

Dangers of big tech

- Social media - tracks where you click, what you buy, who your friends are
- Metaverse - track where you go, what you do, who you're with, where you look, how long gaze lingers, your gait, facial expressions, vocal inflections, vital signs,

Influencing users/participants

- Social media - targeted advertising, curated news feeds,
- Metaverse - will be worse - ultimate tool of persuasion, whole point of VR and AR is to fool the sense, advertising and propaganda will not be flat ads and videos, will be immersive experience
- Virtual product placements - targeted experiences that inject promotional content. Could be indistinguishable from authentic encounters. Could be used for sales or for influencing ideas, propaganda, political

- Virtual spokespeople - AI controlled avatars that engage in promotional conversation, indistinguishable from authentic members of world, have access to data on history, will analyse emotions and adjust tactics to influence

A discussion was had about the risks of organised crime and terrorism in the metaverse by groups who are banned from physical gatherings or social media sites and turn to the metaverse as a place to organise, recruit and promote extremist views, or potentially incite violence.

Discussion # 4 - Metaverse policy and regulation discussion

The group discussed their thoughts on policy or regulation needed for the metaverse. Key discussion points were:

- Governments and the future will need to regulate what is real and what's not. This comes down to identity. There is a need to anchor in the metaverse what is real and what your credentials are.

- We need to start shifting language around the information asymmetry – it is one thing to influence, and another to manipulate. That is where the conversation needs to be. If platform providers know more about you than you do yourself this is not influence, this is manipulation.

- Areas to regulate - security, privacy, safety and digital identity.

- A new Global Online Safety Regulators Network is being launched in November.

- Some young people state that they want to remain anonymous; if it is not anonymous, they don't want to be part of it. Some say I am happy to have an avatar that is not me.

- There is a meeting being set up with the Australian Federal Minister, Ed Husic, and there is a paper in front of the Minister calling for federal government action in setting up a Responsible Metaverse research and forum.

- With regard to anonymity in the metaverse, there is the question of anonymity to who? Some platforms will allow people to specify that they want to be anonymous (meaning to other users) but they usually won't be anonymous to the platform - so the manipulation will still happen.

- Regulation is required around the concept of 'the right to know'. If we ensure the right to know which now also includes 'the right to truth'. This needs to be included in a regulatory approach. This will tell you if someone is an AI avatar - this will be key.

- Unless people know where to go when the harms have been done then the rights are meaningless. At the moment there is a vacuum and there is nowhere to go if a wrong has been committed. Self-regulation is not going to be enough.

- The internet doesn’t have jurisdiction either. Digital policy making across nations is often a bit fractured - each of the regulators sit in different portfolios. A big question is - how do we regulate in a way that is not stifling innovation? How do we make companies approach the metaverse with consideration and hold them accountable? E.g., is going to your local police really going to help you? We need this to happen now as if we try to do this retroactively then it will fail.

- Another question was raised about - is there a ‘right to be forgotten’?
- Indigenous Australians are an area of concern, given the cultural sensitivities around showing pictures/video of those passed. How/who has the right to retire avatars and their biometrics?

- What might happen in the metaverse in terms of harms – what would a Christchurch attack look like in future state? It could be that there are these events where people pay per view, people sit in haptic suits and have a fully immersive experience. The metaverse will bleed into the real world in ways we haven't considered.

- A question was raised - should we regulate haptic suits as well?

- To get a registered IP right in the metaverse - what do you have to give to secure this? To note, the Australian federal government is about to release discussion papers on virtual design, and what this means for design rights.

- Different countries will have different views on regulation. With regard to the metaverse China has a huge investment and most people are optimistic about the metaverse and the potential it has for the digital economy. It may also be a perfect tool for digital oppression and surveillance. There are interesting tensions when looking geopolitically.

- Gaming will lead the development of the metaverse, and that adoption will be greatest in Asia.

- Time is of the essence, and we need to lock in guard rails before business models solidify. It gets very tricky to re-engineer a highly profitable platform to be safer after it has millions or billions of users. So, alongside regulation, how quickly can we get safe practice into emerging metaverse businesses and emerging platforms?

- We have to incentivise companies to do better. One way could be a shared responsibility model - granularly delineating who is responsible for what. So an engineer knows what is my responsibility?

Discussion # 5 - Pathway to impact – the Responsible Metaverse Alliance as a global policy convener

- The Responsible Metaverse Alliance (RMA) may potentially play a role as a global policy convenor.

- The UN CyberCrime treaty is currently being negotiated**.** As a forum, the UN is making those collective agreements that all parties have to comply with. It would need each nation to champion collectively and individually. If we got NZ and Australian foreign affairs teams together, we could petition the UN for some sort of ruling treaty.

- We should seek engagement from the UN.

- The eSafety Commission would like to update its Safety by Design risk assessment tools for the metaverse.

- Some Think Tank members noted that they are at the IGF in Addis at the end of the year.

- Possibility of including a metaverse stream to the proposed AI Inquiry by NSW Government.

Next steps

Next steps included:

1. Sharing of this Metaverse Policy Think Tank Discussion Paper with attendees then a summary to a wider audience
2. Minister Dominello to keep the group updated on the NSW Government AI Inquiry
3. The RMA to approach the Federal Government to fund a Metaverse Experience Centre for policy makers
4. Metaverse Builders Think Tank was held on 18 October 2022 with the aim of gaining input from builders, developers, creators and suppliers to the metaverse, with regard to their views on policy for the metaverse. A summary paper will be released.
5. Metaverse Safety Week is to be held on 10-15 December, led by XSRI- https://metaversesafetyweek.org/

Prepared by Dr Catriona Wallace and Team
Responsible Metaverse Alliance
catriona.wallace@responsiblemetaverse.org
+61 412 181 284

Attendees

Attendees at the Policy Think Tank included:

Minister for Digital and Customer Service, NSW Government - (MP Victor Dominello)
Australian Human Rights Commission
Australian eSafety Commission
Department of Home Affairs - Australian Federal Government
Australia New Zealand Policing Advisory Agency (ANZPAA)
Department of the Prime Minister and Cabinet (DPMC), New Zealand
Information and Privacy Commission NSW
Digital Safety, Toi Hiranga, Regulation & Policy, Te Tari Taiwhenua, Department of Internal Affairs, New Zealand (NZ based)
National AI Centre - CSIRO
Australian Competition & Consumer Commission (ACCC)
NSW Government
NSW Police Force
Crimestoppers
Cyber Security Advisory committee
Tony Blair Institute for Global Change (Singapore)
Unanimous AI (US based)
XR Safety Initiative (USA based)
The Ethics Centre
Centre for Social Impact
Purpose
Reset
Gradient Institute
Smash Delta

Agenda - 5th October 2022

Agenda items included:

1. **Introductory statements**

Dr Catriona Wallace, Founder, Responsible Metaverse Alliance

1) Victor Dominello MP, Minister for Digital and Customer Service
2) Julie Inman-Grant, eSafety Commissioner
3) Nicole Matejic, Kaitohutohu Matua Haumaru Matihiko, Principal Advisor, Digital Safety,Toi Hiranga, Regulation & Policy, Te Tari Taiwhenua, Department of Internal Affairs – New Zealand
4) Kavya Pearlman, Founder XRSI

2. **Discussion re current work in the field**

5) Lorraine Finlay - Human Rights Commissioner
6) Superintendent Julie Boon – NSW Police
7) Rob Forsyth - Director, Crime Stoppers
8) Michael Schwager - Director General, IP Australia
9) Elizabeth Tydd - NSW Information Commissioner

3. **Discussion re risks of the metaverse**

1) Louis Rosenberg Chief Scientist, RMA, Dr
2) Dr Catriona Wallace Founder, Responsible Metaverse Alliance

4. **Discussion re Metaverse policy and regulation**

Group discussion

5. **Discussion - Pathway to impact - global policy convener**

Group discussion

6. **Discussion – next steps**

Dr Catriona Wallace