



Policing in the Metaverse:

Prevention, Disruption, and Enforcement Challenges

Discussion Paper

1 of 3 in 'Policing in the Metaverse' Series

June 2023

CONTENTS

<u>ACKNOWLEDGEMENTS.....</u>	<u>3</u>
<u>INTRODUCTION.....</u>	<u>4</u>
<u>CRIMES IN THE METAVERSE.....</u>	<u>5</u>
<u>CHALLENGES FOR POLICING IN THE METAVERSE.....</u>	<u>6</u>
<u>National Legal and Regulatory Frameworks are Not Metaverse-Ready.....</u>	<u>6</u>
<u>Lack of International Agreements Inhibit Law Enforcement Coordination.....</u>	<u>7</u>
<u>Technical Expertise of Law Enforcement.....</u>	<u>9</u>
<u>Safety (and Human Rights) by Design.....</u>	<u>9</u>
<u>Public Education, Awareness and Digital Literacy.....</u>	<u>11</u>
<u>CONCLUDING REMARKS AND NEXT STEPS.....</u>	<u>12</u>
<u>SUMMARY OF OPPORTUNITIES.....</u>	<u>13</u>
<u>REFERENCES.....</u>	<u>15</u>
<u>APPENDIX.....</u>	<u>16</u>

ACKNOWLEDGEMENTS

RMA acknowledges the traditional owners of the lands we work from in Australia, and pay our respect to elders past and present. We thank Aboriginal and Torres Strait Islander people for their continued knowledge, wisdom and connection to the unceded lands and waters that we now raise our families and share in community on. Always was, and always will be, Aboriginal Land.

The RMA is an organisation built on collaboration with partners from many sectors and nations. In particular, we want to acknowledge those who have committed their time, expertise and wisdom to this work. In particular, the individuals who contributed and/or presented their work which sparked such valuable discussion at this think tank:

Speakers: **Dr Catriona Wallace**, Founder, Responsible Metaverse Alliance
 Wookyung Jung, Policy Analyst, Executive Directorate Technology and Innovation Interpol
 Dr Justin Ellis, Senior Lecturer in Criminology, The University of Newcastle
 Acting Commander Brad Marden, Cybercrime Operations, Australian Federal Police

We also acknowledge the many other individuals and organisations who participated in and/or contributed to this think tank.

INTRODUCTION

The Metaverse is already having an impact on how we connect, behave and interact, and the Responsible Metaverse Alliance (RMA) was established to nurture the optimism around the potential of the Metaverse to improve lives and unleash new opportunities for creativity, community-building and learning. All technologies of course come with risk and the Metaverse poses unique challenges for ensuring these immersive environments are safe and that the rights of users are protected.

Around the globe, there are already almost half a billion people regularly using the Metaverse - and 8 in every 10 are young people. With law enforcement agencies already observing a groundswell of criminal activity in these immersive environments, the global nature of the Metaverse poses immediate and unique safety challenges for agencies and technology companies in protecting users. Just like in the physical world young people, women, minorities and the vulnerable are most at risk of falling victim to criminal activity, and it was for this reason that RMA has committed to addressing Policing in the Metaverse as a priority focus.

With the rapid advancement in technology, artificial intelligence, and uptake of the Metaverse, we are at significant risk of repeating the mistakes of the Internet 2.0 era by not prioritising user safety and falling into the pattern of regulatory catch-up that no government has yet proven successful in. The responsibility for this lies with many stakeholders, from developers incorporating safety-by-design best practice, to law enforcement being prepared and resourced appropriately, to users being aware of their rights and the risks. And with safety being both an ethical responsibility and a commercial imperative, we saw the need to facilitate and create new spaces that bring together the best minds from all sectors of society, to discuss, collaborate and tackle the challenge at hand.

On the 7th of June 2023, the Responsible Metaverse Alliance and partners held the first of three online Think Tanks focused on Policing in the Metaverse. Bringing together a range of experts representing international law enforcement agencies, Australian Commissions, policy makers, safety regulators and civil society, the discussion centred around the unique dynamics and challenges that the Metaverse poses for law enforcement. The stated objective of the Policing in the Metaverse Think Tank series is to identify, articulate and discuss:

- 1) the potential crimes in the Metaverse
- 2) policing jurisdictions
- 3) the role that police services and law enforcement agencies should play and;
- 4) what regulation is required to keep people safe.

This discussion paper is the output of that conversation and is intended to surface the key themes, articulate the various crimes and the new dynamics of those acts in the Metaverse, and to outline the challenges for law enforcement in addressing, mitigating and preventing such crimes. The primary intention is that this discussion paper can serve to generate input from the broader community of Metaverse stakeholders.

The task of building and maintaining a safe Metaverse requires a multi-disciplinary and collaborative approach. And the responsibility of keeping users safe falls unevenly across a number of stakeholders, each with a distinct role to play. Those stakeholders and their broad responsibilities, as were discussed, include:

- **Local, national and international law enforcement agencies** - policing and enforcement
- **Governments** - policy and legislation
- **Regulators** - enforcement and setting of industry codes
- **Tech companies / platforms** - safety by design , accountability for crimes enabled by their products
- **Civil society** - education, awareness
- **Community of users** - awareness

CRIMES IN THE METAVERSE

Law enforcement agencies are already working to address crimes in the Metaverse, and while many of these crimes mirror those in both the digital and the physical world, the Metaverse enables them to be committed in new ways through new methods and tactics.

The immersive nature and increased anonymity of the Metaverse both connects people in new and exciting ways, while inversely disassociating people from the real world and the impact of their behaviour and actions. This combined with the lack of regulation and oversight results in a new dynamic of criminal harm where individuals feel more empowered to engage in criminal or unethical behaviour, while simultaneously disempowering victims who are less able to seek redress or justice. Interpol has created a global Metaverse expert group (I-MEG) working to develop the first taxonomy of crimes in the Metaverse, which will serve to provide a guiding framework for coordination and collaboration between law enforcement agencies around the world. While the taxonomy is a work in progress, Wookyung Jung from Interpol shared the broad categories of crimes - many of which were discussed during this Think Tank, and include:

- *Financial crime*
- *Crimes against children*
- *Assault and sexual violence*
- *Terrorism related crime*
- *Acts intended to induce fear or emotional distress*
- *Crimes against public safety*
- *Cybercrime*
- *Coercion*
- *Property crime*
- *Intellectual property crime*

Currently, law enforcement agencies are typically seeing the extension of crimes already committed on the internet, brought into the Metaverse. And most are deploying existing approaches and methods used to counter cybercrime, which provides somewhat of a foundation of learnings and insights from that experience, but exposes numerous gaps in their readiness for policing in the Metaverse.

The rapid uptake of the immersive technologies of the Metaverse is occurring alongside new developments in artificial intelligence. While this provides endless exciting possibilities for users, it simultaneously enables new types of crime, which governments and the law enforcement community are not at all prepared to address. In our discussion there was mention of such anticipated-but-not-yet-seen crimes, which could include the following among others:

- I. AI compromising privacy or security by correctly inferring sensitive information gleaned from within the Metaverse, e.g. biometric data and emotive response, Gen-AI manipulation through avatars and with the use of API plug-ins.
- II. Theft of virtual property, e.g. virtual real estate, avatars etc
- III. Human-like interaction with AI systems and interfaces that amplify opportunities for user nudging, deception and manipulation (e.g. fraud, scams, radicalisation etc), including through the use of stolen identities, or personalised immersive experiences
- IV. Virtual, immersive and AI-powered deep fakes

There are other crimes that were mentioned but not discussed in detail, including the particular dynamics of crimes in the 'Darkverse'. However these are not included in this paper and require further research and exploration to adequately address.

CHALLENGES FOR POLICING IN THE METAVERSE

There are a significant number of challenges facing law enforcement agencies in the Metaverse, and it is clear that these cannot be overcome by adopting the same approach that is taken to policing crimes in the physical world. This point is relevant for both how law enforcement approaches the detection of crimes, as well as how legislation is designed to future-proof protections for immersive and emerging technologies.

It is also important to recognise that, as is the case with other forms of cybercrime, law enforcement needs to have a strong focus on the *prevention* and *disruption* of criminal activity. Prosecuting cybercrime is slow, difficult under existing legislation, and often requires resourcing beyond the reach of most people - and so a focus on disruption and prevention will be key to policing efforts in the Metaverse. It is broadly accepted that to overcome the challenges outlined here, a more holistic approach is required - one that considers regulation, prevention, disruption, and enforcement. These are outlined under the following challenges:

1. National Legal and Regulatory Frameworks are Not Metaverse-Ready
2. Lack of International Agreements Inhibit Law Enforcement Coordination
3. Technical Expertise of Law Enforcement
4. Safety (and Human Rights) by Design
5. Public Education, Awareness and Digital Literacy

CHALLENGE 1:

National Legal and Regulatory Frameworks are Not Metaverse-Ready

There is broad acknowledgement of the limitations of existing criminal law to prevent crimes in the Metaverse. Legislation and regulation addressing crimes in the digital sphere are already outdated, and amendments are unlikely to keep pace with the development and uptake of the Metaverse. This places significant pressure on policymakers to pass effective legislation and regulations that are future-proofed for the ongoing development of Metaverse and artificial intelligence technologies. Designing and enacting a legislative framework that can address crimes in the Metaverse must be a top priority, as it not only enables law enforcement and prosecution, but also serves as foundations to inform better industry standards and principles.

Much of the crime that is committed through the internet already goes unaddressed, which is in part due to the impunity of platforms from the criminal activity that occurs on their platforms -

best known through the protections under Section 230 of the United States' Communications Decency Act Of 1996.

OPPORTUNITY

There is a clear opportunity for governments to avoid relying on reactionary legislation after crimes have been committed and harm caused to victims, and to instead get ahead of crimes in the Metaverse through:

1. **Definitions** - there is a need for establishing consistent and shared definitions of 'hate speech' and 'harassment' - which are already inadequate for addressing online hate speech - and in particular should include other forms of 'expression' like touching, use of symbols etc in order to make them applicable to potential actions in the Metaverse.
2. **Balancing Freedom of Expression and Dignity** - providing clarity on the balance between freedom of expression and an individual's inherent right to dignity.
3. **Platform Accountability** - Regulation needs to consider not only perpetrators of crimes but also the platforms and companies that enable or facilitate those crimes - even if done so inadvertently. Put simply, regulating that considers the accountability of platforms and their role in designing and maintaining products with adequate safety features.
4. **New Legislation** - in the known gaps including:
 - a. Virtual property rights (eg avatars and virtual real estate);
 - b. Virtual identity verification;
 - c. Trespassing in the Metaverse;
 - d. Virtual or AI representation of children and/or the generation of child exploitation material (as demonstrated under current Australian laws but not reflected elsewhere);
 - e. Smart contracts - many of which are poorly built and contain many vulnerabilities that are already being exploited for financial gain.

CHALLENGE 2:

Lack of International Agreements Inhibit Law Enforcement Coordination

There was a strong perspective amongst many participants that while there are already challenges and policy gaps between federal and state level legislation within nation states, a global regulatory framework is likely an unrealistic goal. However, there are crucial international agreements that are required to enable law enforcement to collaborate in policing crimes in the Metaverse. Chief amongst these include agreements that address jurisdictional prominence and enable coordination across jurisdictions. There are two key dimensions to this challenge, the first is that

“The challenge is attribution, [which] becomes about data sharing and information connections. Traditional law enforcement methods of sharing information are glacial [compared to] the way offending happens”

- Participant quote

while jurisdictional prominence is already a challenge in policing crimes on the internet, it practically does not apply in the Metaverse because the immersive technologies upend existing definitions and concepts of ‘place’. This makes attribution of Metaverse crimes particularly difficult, and is further compounded by the second dimension in that the necessary information is not readily available to law

enforcement agencies - as it is typically held by other governments, regulators, or platforms based in other countries. There is a significant challenge in establishing effective information and data sharing agreements between law enforcement agencies (and platforms) that can establish attribution rapidly while responsibly protecting user data and privacy - and particularly the use of such data by malicious governments. Relevant here is the approach of the Australian Centre to Counter Child Exploitation, which prioritises strong effective relationships with international counterparts to coordinate in disruption efforts, share new technology and techniques, among other collaboration.

Further to this challenge, there is a general misperception that the Metaverse will not facilitate strong interoperability between platforms, however expert participants expressed that virtual spaces will undoubtedly evolve to incorporate a number of platforms and products. This will make accountability of particular platforms difficult as it may not be clear ‘where’ someone is in such spaces. Additional to this ‘horizontal’ interoperability between platforms, the ability of different stakeholders to navigate across the virtual, digital and physical worlds will be critical to their effectiveness. This conceptualisation of ‘vertical’ interoperability is most apt in relation to the need for cooperation between law enforcement and platforms. In the first instance, developers require insights from law enforcement on how their platforms and products can be used to commit crimes, to inform the incorporation of safety design features. And further, it is clear that law enforcement cannot effectively investigate crimes without the assistance of the platforms - particularly in establishing the means of cooperation that ensures privacy is protected and government overreach and surveillance is prevented.

OPPORTUNITY

There is considerable work to be done to establish effective data and information sharing processes for law enforcement agencies across jurisdictions. International agreements will be necessary, and will need to be backed by strong domestic regulation that is enforceable and reconceptualises ‘place’ in investigating crimes conducted in interoperable virtual spaces.

Further there is a need for agreements that enable greater coordination with platforms in ways that are transparent and accountable.

CHALLENGE 3:

Technical Expertise of Law Enforcement

For law enforcement to be able to effectively identify and investigate Metaverse crimes, agencies and officers need to be able to navigate the Metaverse, and that requires an understanding of the technology and the ways in which people use it. Numerous dimensions to this challenge have been raised, though a key framing has been through the acknowledgement that criminals typically ‘think creatively’ to deceive victims and evade law enforcement. And that they will be able to do this because of their advanced understanding of the environment within which they’re operating. Without law enforcement agencies being equipped with a thorough understanding of the technology and the ways in which users engage in the Metaverse, ‘criminals will leapfrog law enforcement everytime.’ So while legislation relating to policing in the Metaverse needs to provide greater powers to focus on detection and disruption of crimes alongside enforcement, there is a need to resource agencies with the creative, strategic and innovative capabilities and thinking that take into consideration the design and environment of the Metaverse.

“the creativity of our offender base well exceeds that of the ability of law enforcement to respond”

- Participant quote

Without law enforcement agencies being able to demonstrate a sophisticated understanding of the Metaverse in their policing activities, we can expect significant public and media scrutiny which will be amplified by their own broader lack of understanding of the technologies - creating a likely scenario where the most adept individuals are those committing crimes.

In relation to the uptake of artificial intelligence, it is also recognised that there is a need for agencies to explore the potential of such technologies in detecting crimes and supporting subsequent policing.

OPPORTUNITY

Law enforcement agencies need to be investing in training and resourcing of personnel in the Metaverse, including nurturing better and responsible use of new technologies - like artificial intelligence - in assisting to detect and police crimes in the Metaverse.

CHALLENGE 4:

Safety (and Human Rights) by Design

The task of law enforcement in policing the Metaverse will be heavily influenced by how safe the environments and products are designed. There is currently no assurance for users that Metaverse and AI products are going to be built with the necessary guardrails, controls or restrictions that can ensure user safety. This poses a significant threat with the potential to accelerate and amplify

the harms of crimes committed in the Metaverse, particularly when the technology is deployed at scale.

To ensure Metaverse products and platforms are designed with user safety in mind, developers need established guidelines and standards for how to do that effectively. While there are clear needs for the inclusion of particular safety features like built-in reporting and support mechanisms for users who have fallen victim to criminal activity, the necessary design frameworks and guidelines should encapsulate the entire development process, from contracting through to deployment and beyond.

Another key component of safety by design is in companies also providing transparency around decision-making, so that it is clear to users and regulators who in the process is making design decisions, and informed by what considerations and factors. This helps ensure there is accountability for those decisions with senior management, while also providing appropriate incentives for developers and designers to make their products safe.

The recent white paper from Standards Australia - and authored by RMA and XRSI, outlines proposed industry standards to prevent targeted influence and manipulation in the Metaverse,

“This technology isn’t there for its own sake. It’s meant to be there to make our lives better. And ensuring that it enhances human rights rather than risks or undermines them is a key part”

- Participant quote

which include the right to: i) experiential authenticity; ii) emotional privacy; iii) behavioural privacy; and iv) human agency. The paper outlines additional areas for standards development in Australia that are also applicable in other jurisdictions that include focusing on Responsible AI aspects of Metaverse platforms and extending the Responsible AI framework and Child Safety Standards.

Going beyond Safety-by-Design, there is also a need to ensure the human rights of users also avoids being a conversation after harm is committed, which can be mitigated by furthering the development and thinking of human-rights-by-design. Both of these approaches are practically absent in the current approach to the development of these products.

OPPORTUNITY

Establish better processes that incorporate safety-by-design and human-rights-by-design from the start and throughout the development and deployment of Metaverse products. As well as ensuring transparency around decision-making in relation to the use of artificial intelligence and algorithms.

CHALLENGE 5:**Public Education, Awareness and Digital Literacy**

While the accountability for crimes committed in the Metaverse - along with the responsibility for policing them - sits with developers, regulators, government and law enforcement, there is also a need to ensure users are aware of the risks and informed on actions that can be taken. With the creation of new technologies and new subsequent crimes, it is often the case that people are not even aware that they are a victim of a crime.

Awareness and education campaigns should be mandated by governments to ensure they - and importantly the platforms - are responsible for user awareness around how to keep themselves safe where crimes evade safety features. This includes awareness of how to access support mechanisms and to report crimes to law enforcement in simple and fluid ways. While these initiatives are required for all demographic groups, they require adaptation to particular groups and situations. For example, most young people tend to have very high awareness of the risks in online spaces, but often lack the tools or are not empowered to keep themselves safe. This falls broadly under 'digital literacy' but importantly that term has different implications and connotations with different audiences.

OPPORTUNITY

Requiring platforms and resourcing governments to develop the tools and resources - tailored for different demographics - to help users navigate the Metaverse safely. These should be developed in partnership with civil society, and should include education on the potential harms, a user's rights, and their avenues for redress and support.

CONCLUDING REMARKS AND NEXT STEPS

The hard truth that has emerged from this discussion is that we are not prepared to provide a safe Metaverse for users, particularly for children and the vulnerable. There are glaring gaps in existing legislation, law enforcement lacking the technical expertise and capabilities to do their job well, through to designers and developers lacking the guidance needed to inform the design and development of safe Metaverse products. We also have a public that lacks the awareness or knowledge of the risks. The challenge is significant.

The silver lining is that there already exists a network of individuals, companies, organisations and agencies that are cognisant of these challenges and are beginning to undertake the necessary collaborative and multidisciplinary approach required. The RMA is now planning the next two Think Tanks in this series on 'Policing in the Metaverse', and we are eager for recommendations from all sectors of the community, industry, law enforcement and government, to inform our focus as we progress.

We hope that this Discussion Paper as a result of the first Think Tank will stimulate further discussion and start to mobilise actions towards some of the recommendations made.

We need a safe Metaverse that meets the promise of these technologies to improve lives and strengthen communities.

SUMMARY OF OPPORTUNITIES

All of the opportunities outlined in this Paper signal the urgent opportunity that currently exists for governments and law enforcement to get on the front foot, and to avoid playing a reactive catch up as has been the case with Internet 2.0.

1. National Legal and Regulatory Frameworks are Not Metaverse-Ready

- 1. Definitions** - there is a need for establishing consistent and shared definitions of 'hate speech' and 'harassment' - which are already inadequate for addressing online hate speech - and in particular should include other forms of 'expression' like touching, use of symbols etc in order to make them applicable to potential actions in the Metaverse.
- 2. Balancing Freedom of Expression and Dignity** - providing clarity on the balance between freedom of expression and an individual's inherent right to dignity.
- 3. Platform Accountability** - Regulation needs to consider not only perpetrators of crimes but also the platforms and companies that enable or facilitate those crimes - even if done so inadvertently. Put simply, regulating that considers the accountability of platforms and their role in designing and maintaining products with adequate safety features.
- 4. New Legislation** - in the known gaps including virtual property rights (eg avatars and virtual real estate); virtual identity verification; trespassing in the Metaverse; virtual or AI representation of children and/or the generation of child exploitation material (as demonstrated under current Australian laws but not reflected elsewhere); smart contracts - many of which are poorly built and contain many vulnerabilities that are already being exploited for financial gain.

2. Lack of International Agreements Inhibit Law Enforcement Coordination

There is considerable work to be done to establish effective data and information sharing processes for law enforcement agencies across jurisdictions. International agreements will be necessary, and will need to be backed by strong domestic regulation that is enforceable and reconceptualises 'place' in investigating crimes conducted in interoperable virtual spaces. Further there is a need for agreements that enable greater coordination with platforms in ways that are transparent and accountable.

3. Technical Expertise of Law Enforcement

Law enforcement agencies need to be investing in training and resourcing of personnel in the Metaverse, including nurturing better and responsible use of new technologies - like artificial intelligence - in assisting to detect and police crimes in the Metaverse.

4. Safety (and Human Rights) by Design

Establish better processes that incorporate safety-by-design and human-rights-by-design from the start and throughout the development and deployment of Metaverse products. As well as ensuring transparency around decision-making in relation to the use of artificial intelligence and algorithms.

5. Public Education, Awareness and Digital Literacy

Requiring platforms and resourcing governments to develop the tools and resources - tailored for different demographics - to help users navigate the Metaverse safely. These should be developed in partnership with civil society, and should include education on the potential harms, a user's rights, and their avenues for redress and support.

REFERENCES

Australian Centre to Counter Child Exploitation (2022), '*Strategic Plan 2022 – 2026*'
<https://www.accce.gov.au/sites/default/files/2022-09/ACCCE%20Strategic%20Plan%202022-26.pdf>

Australian Human Rights Commission, '*Human rights at your fingertips: International Covenant on Civil and Political Rights*'
<https://humanrights.gov.au/our-work/commission-general/international-covenant-civil-and-political-rights-human-rights-your>

Metaversed, '*The Metaverse Reaches 400m Monthly Active Users*'
<https://www.metaversed.consulting/blog/the-metaverse-reaches-400m-active-users>

Standards Australia (2023), '*Metaverse Standards White Paper*'
https://www.standards.org.au/getmedia/beb254c9-fd95-4602-bc7b-8de12ba91287/H2_3061_Metaverse_report.pdf.aspx

United States Department of Justice, '*Department of Justice's Review of Section 230 of the Communications Decency Act Of 1996*'
<https://www.justice.gov/archives/ag/departement-justice-s-review-section-230-communications-decency-act-1996>

APPENDIX

Think Tank: Policing in the Metaverse Series

#1 Crimes in the Metaverse

7th June 2023 | 10am - 11.30am (AEST) | 90 mins | Virtual event

Participants: International law enforcement agencies, policy makers, safety regulators and civil society.

Objective: To identify, articulate and discuss:

- 1) the potential crimes in the metaverse
- 2) policing jurisdictions
- 3) the role that police services and law enforcement agencies should play and;
- 4) what regulation is required to keep people safe.

This first Think Tank will focus on identifying the crimes that may occur in the metaverse and relevant policing jurisdictions.

Overview

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). It is estimated that there are 470 million users of the metaverse currently, mostly children and young people. These virtual worlds bring great potential benefits, however that are largely unregulated, and have few to no laws or regulations or oversight, and certainly no police stations. So, what happens when a crime is committed in a virtual world? What are the crimes that can occur in the metaverse? How do people access policing? What do policing organisations need in order to be equipped to effectively police the metaverse? And whose jurisdiction is the metaverse?

This first Think Tank will focus on ‘crimes against a person or group’ - intentionally excluding administrative or civil crimes - and based on research and consultation, we have identified the following crime categories that may be perpetrated in the metaverse and will form the basis for our conversation:

1. Child exploitation and extortion
2. Promulgation of harmful ideologies (eg organised terrorism, radicalisation)
3. Harassment (eg hate speech and threats of violence)
4. Transference of illicit commodities such as drugs and firearms
5. Foreign interference

Agenda

10:00 - 10:10am <i>10 mins</i>	Opening + Acknowledgement of Country Introducing the session and its focus, introducing speakers, housekeeping, gaining recording permission. Chatham House Rules apply.
10:10 - 10:30 am	Speaker Round Crimes in the metaverse

<p>20 mins</p>	<p>Speakers will present insights into crimes in the metaverse.</p> <ol style="list-style-type: none"> 1. Dr Catriona Wallace, Founder Responsible Metaverse Alliance. 2. Wookyung JUNG, (Policy Analyst, Executive Directorate Technology and Innovation, INTERPOL. 3. Dr Justin Ellis Senior Lecturer in Criminology, The University of Newcastle 4. Detective Superintendent Bradley Marden, Cybercrime Strategy, Cyber Command, Australian Federal Police.
<p>10:30 - 11:10 am 40 mins</p>	<p>Group Discussion Crimes in the Metaverse</p> <p>Building on the insights from our speakers, we will have a facilitated conversation exploring the dynamics of crimes occurring in the metaverse, with contributions from participants on work or research already underway.</p> <p>Topics to expand on include:</p> <ol style="list-style-type: none"> 1. Child exploitation and extortion 2. Promulgation of harmful ideologies (eg organised terrorism, radicalisation) 3. Harassment (eg hate speech and threats of violence) 4. Transference of illicit commodities such as drugs and firearms 5. Foreign interference <p>Discussion prompts:</p> <ol style="list-style-type: none"> 1. What crimes against persons have not been discussed here so far? (beyond child exploitation/extortion, promulgation of harmful ideologies, foreign interference, transference of illicit commodities) 2. From an enforcement perspective, what are the new dynamics of these crimes when committed in the metaverse? 3. What worries you most about how crimes may be committed in the metaverse?
<p>11:10 - 11:25 am 15 mins</p>	<p>Group Discussion #2 Policing Jurisdictions in the Metaverse</p> <p>Discussion prompts:</p> <ol style="list-style-type: none"> 1. How is law enforcement in the metaverse defined? Does it differ between online and offline policing? And how does interoperability between the virtual, digital and physical worlds in policing processes work? 2. What current policing work and/or research is currently happening in the field? And what international collaboration exists? 3. Without international boundaries, how do we need to think about jurisdictions for policing in the metaverse?
<p>11:25 - 11:30 am 5 mins</p>	<p>Wrap Up</p> <p>Summary of the key points and next steps - Dr Catriona Wallace</p>