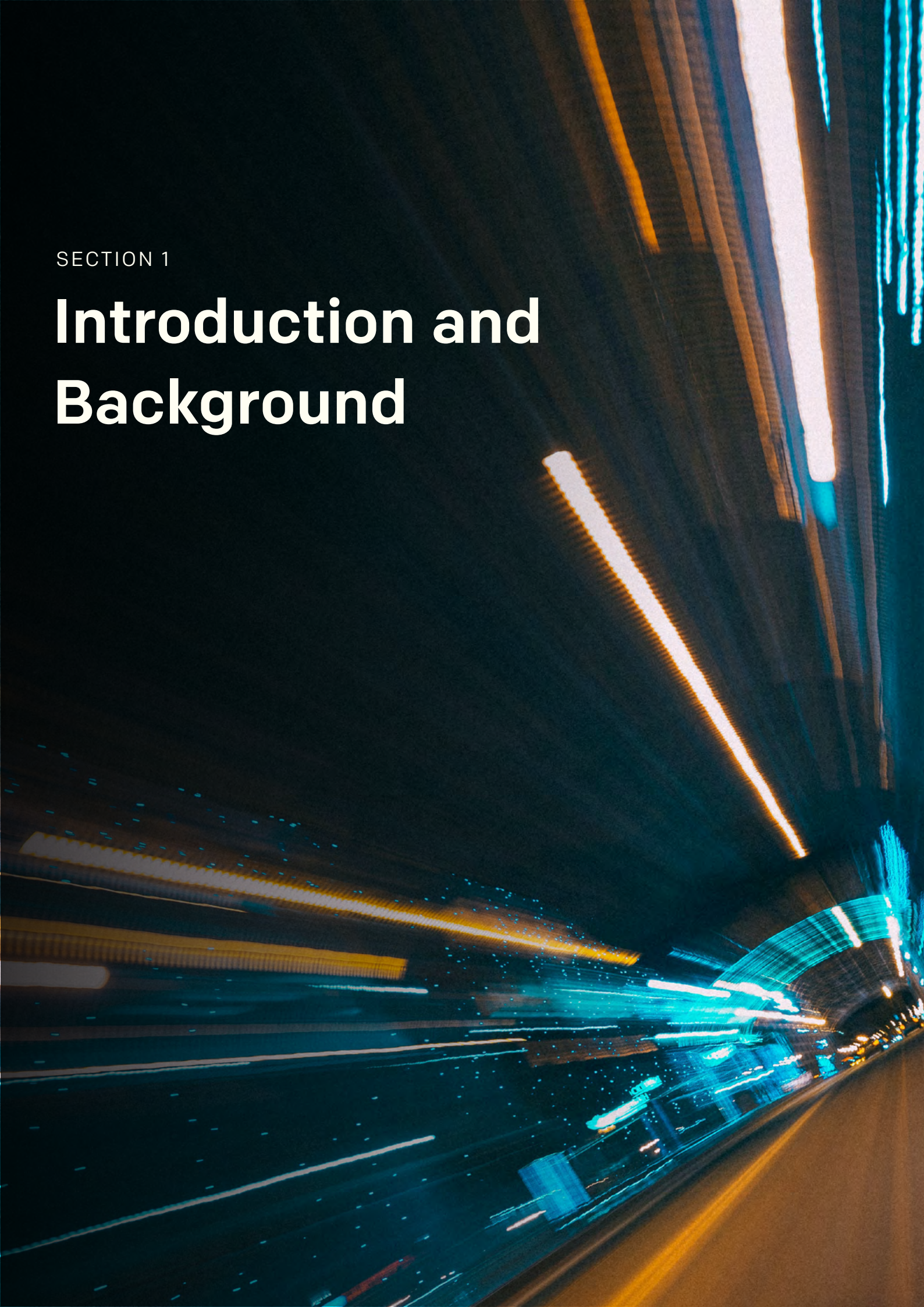
UNITED ARAB EMIRATES
MINISTER OF STATE FOR ARTIFICIAL INTELLIGENCE,
DIGITAL ECONOMY & REMOTE WORK APPLICATIONS OFFICE

WHITEPAPER

Responsible Metaverse Self-governance Framework

Contents



SECTION 1

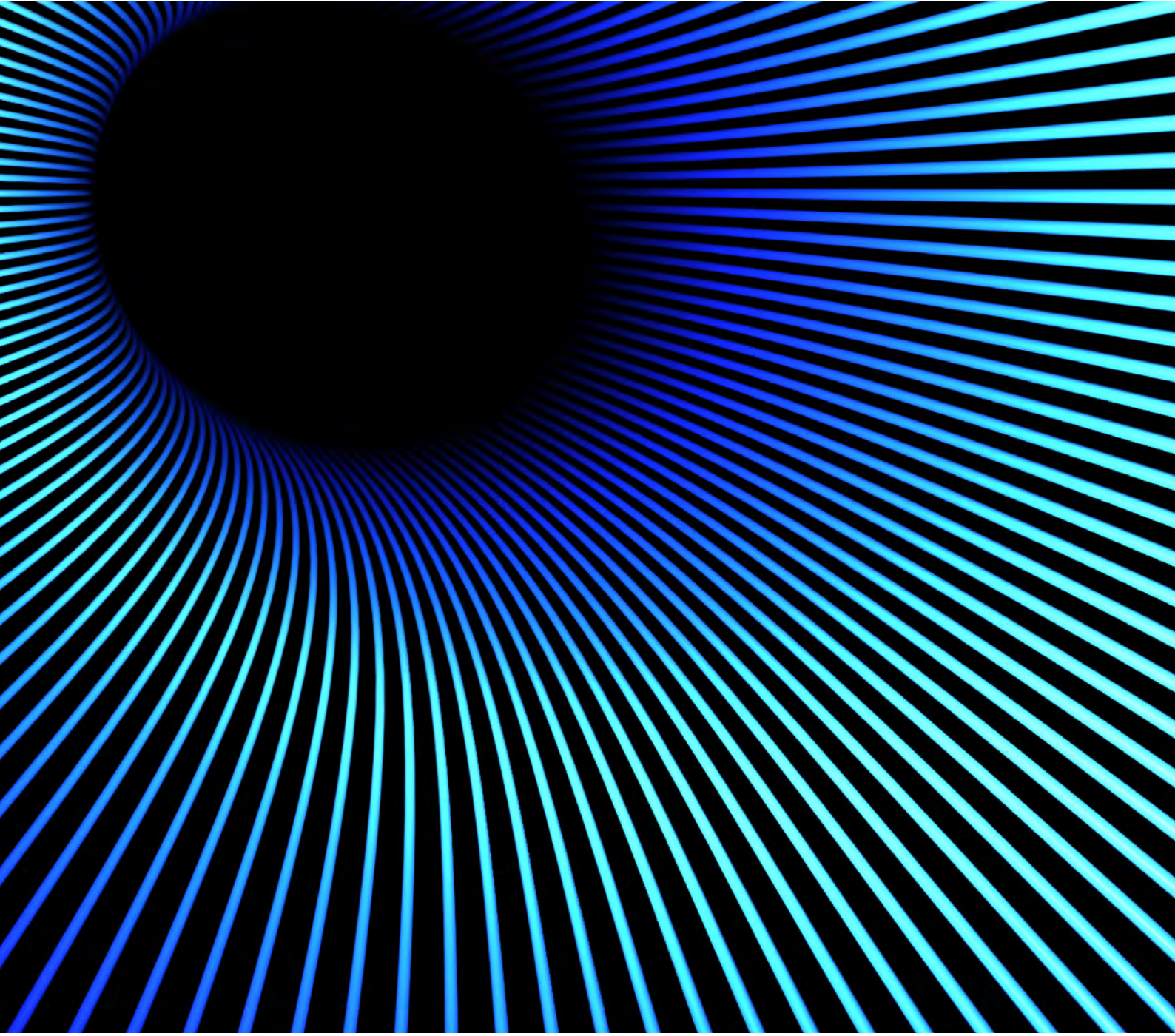
Introduction and Background

Introduction

Post-COVID 19 pandemic, there has been a flurry of activities in the emerging metaverse. It has been estimated that until mid-2022 there have already been investments of more than US$ 120 billion into the metaverse - more than double the US$ 57 million invested in 2021.[1] Interestingly, in addition to large technology companies, governments are also actively participating in this space. With the increasing engagement of both public and private sector, the metaverse has emerged as one of the biggest new growth opportunities across several industries for the next decade and it is estimated that by 2030, the metaverse could generate 4 to 5 trillion US$.[2] The Dubai Metaverse Strategy estimates the metaverse will add US$4 billion to its economy and support 42,000 jobs by 2030.[3]

However, in order for the metaverse to reach its ever-growing potential, there is a need to have in place real-world controls to protect users and other stakeholders operating in the metaverse. That said, given that the metaverse is technically borderless, there are complex legal and regulatory challenges. This is amplified by the lack of unified and uniform explicit frameworks and regulations at the global level that regulates the metaverse and metaverse enabling technologies. Moreover, given the revolutionary nature of the metaverse, it will take time for governments to keep pace with the technological innovations in this space. This implies a lack of governance over the metaverse which poses concerns across diverse areas such as data security, privacy, online harm, user safety, interoperability, digital well-being, addiction, intellectual property, open access to the metaverse, consumer protection, advertising technology, content moderation, identity theft and fraud.

1 Value Creation in the Metaverse, McKinsey, June 2022
2 Value Creation in the Metaverse, McKinsey, June 2022
3 Dubai Metaverse Strategy, July, 2022



Agile Nations Metaverse Working Group

Recognising the need to address the immediate and multifaceted challenges in metaverse governance, the Agile Nations chaired by the United Arab Emirates' Prime Minister's Office set up the Agile Nations Metaverse Regulation Working Group in April 2022 led by the Minister of State for Artificial Intelligence, Digital Economy and Remote Work Applications Office of the United Arab Emirates. The objective is to identify common minimum self-regulatory principles and standards for responsible use and operation in the metaverse. The Agile Nations is an intergovernmental network established in December 2020 with support from World Economic Forum (WEF) and the Organisation for Economic Co-operation and Development (OECD) to bring governments and industry together to collaborate on creating a global regulatory environment that allows innovation to flourish while upholding protections for individual citizens, societies, companies and the environment. The network comprises the United Arab Emirates (UAE), United Kingdom (UK), Canada, Denmark, Italy, Japan and Singapore and is currently chaired by the UAE.

Objective

The objective is to publish a whitepaper that establishes common minimum self-regulatory principles for responsible use in the metaverse.

Methodology

This paper is being issued pursuant to a consultation process with diverse and key industry stakeholders via a feedback questionnaire. The purpose of the questionnaire was to consult and receive insights/ feedback from the private sector / government / international agencies to identify the critical issues that need be considered for regulation in the metaverse, sharing their experience in developing or co-developing policies and guidelines on the metaverse (if any) and providing recommendations. The questionnaire included questions about the existence, robustness and implementation of the existing legal and regulatory framework that underpins the metaverse and coordination required to be developed internationally to successfully regulate the metaverse. These questions were designed to begin the journey towards identifying and establishing common minimum self-regulatory principles for responsible use in the metaverse to be documented within a policy.

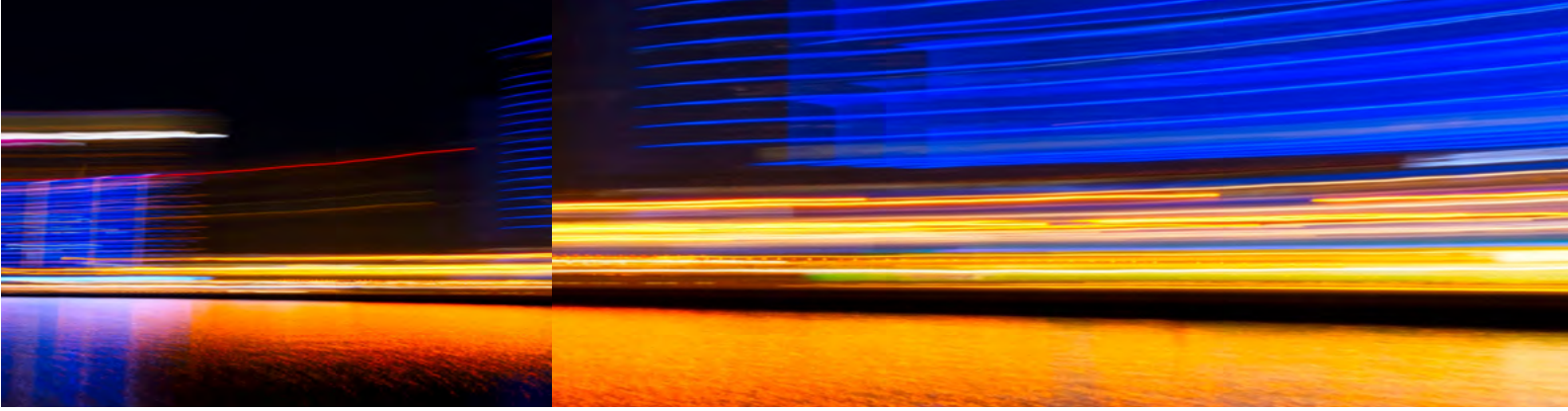
The consultation process provided us valuable insights on the critical issues to be tackled within the mandate and forms the basis of this paper and the proposed self- regulatory principles (as enumerated in Section 5 below).

What is the 'metaverse', its significance and challenges?

The metaverse may be considered to be an overarching platform like the Web. The metaverse is a massively scaled, connected network of persistent virtual spaces (2D and 3D) that augments, facilitates, and coordinates with the real world in real time.[4] From a technology perspective, we are yet to evolve from the real world to the virtual world with the same level of granularity where huge populations can access it simultaneously. For this to happen, the infrastructure technology and standards on data transferability need to change. In the metaverse, people would represent themselves as they want via one or several digital avatars. Through these representations, they could interact socially, economically, and experientially in this space. Whether they wish these identities to be aligned or remain fragmented is a choice that may not always be desirable. Having said that, the metaverse is interconnected such that it allows for the concurrent and seamless transfer of data in both directions allowing users access to and participation in customisable and/or co-created services and experiences, with concurrent rights and obligations across both virtual and real worlds. This seamless experience will need the continuity of data, which will meld permissions granted between online and offline identity(ies), history, entitlements or assets, objects, communications and payments. An example of a governance challenge is as the user moves from a child-centric metaverse space to a more adult or public area or vice-versa and whether the guardrails created are sufficient.

The defining quality of the metaverse is the sense of "presence." With time, more people will be represented virtually, living parts of their daily lives online with legal digital representations using avatars or other instruments. This shift will change the way we view the world and also change the way we are governed. The metaverse will result in the seamless convergence of our physical and digital lives, resulting in virtual communities that replicate

4 Ball, M. (2022), The Metaverse: And How It Will Revolutionize Everything; Stephens et al. (2022). Metaverse and Governance. IEEE SA; Garner (2022). What Is a Metaverse?



their real-world where individuals can work, play, learn, relax, transact, access specialised services, and socialise.

The metaverse may be centralised[5] or decentralised[6] depending on the use case (for example, high security, highly specialised, or sensitive data may be more likely available in a closed-loop metaverse space). Hence, this suggests that the metaverse may also have fragmented, isolated spaces for security, sovereignty, or other reasons.

Another key concern related to the metaverse is the wide range of technology that can enable equity in participation. This extends across a diverse and varied technology stack that operates at multiple levels. The technologies that enable the metaverse include artificial intelligence (AI), hardware like virtual reality (VR), augmented reality (AR) sets, sensors in internet of things (IoT), haptics, microphones, and wearables; infrastructure like Web 3.0 (4G, 5G, or 6G), computing devices, data servers, cloud, data farms, or specialised software like edge computing, blockchain technology applications, and content development. Soon, some of those technologies will also be neural interfaces of other biological materials. Most respondents to our feedback questionnaire agree that the metaverse should be technology agnostic concerning access. So whether the individual chooses a computer, laptop, mobile, VR glasses, wearable or game console, the individual should still be able to interact safely and consistently with the metaverse (the individual would decide how immersive they want the experience to be).

Whilst there is a perspective that the metaverse needs 3D persistent virtual worlds[7], there remains a continuing need to integrate with 2D technologies and offline activities through IoTs. As the metaverse evolves, Web 3.0 and blockchain technologies will offer more decentralisation and autonomy for users relative to Web 2.0. As part of this evolution, it is anticipated that digital assets will form an integral part of the Web 3.0 ecosystem as participants increasingly access digital goods and services virtually.

In terms of development, whereas the core technologies exist and are being deployed in silos in use cases spanning multiple industries, the full extent of development may still be 5-10 years away. Hence, the development of the metaverse may be seen as a continuum. Typically, organisations are more likely to embrace the metaverse at the lower end of the continuum (typically independent virtual spaces such as digital twins and virtual games) with a push to have more interconnected, decentralised spaces.

In the context of the above background, the challenge moving forward is to determine which of the existing regulations apply to the metaverse, what are the gaps in regulations due to emergence of new technologies, and how the regulations may be enforced in the real world. Hence, there is a need for an open dialogue for the co-creation of governance frameworks that are universal and self regulatable without limiting the opportunities the metaverse may provide. As the OECD states in its report, How's Life in the Digital Age?: Opportunities and Risks of the Digital Transformation for People's Well-being, an interim solution may be to use digital security incidents to measure risk until we have sounder national digital policies and a more mature digital society.[8]

5 Associated with Web 2.0.
6 Associated with Web 3.0, where users should have more autonomy.
7 European Parliament (2022), Think Tank. Metaverse: Opportunities, risks and policy implications, https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733557
8 OECD (2019), How's Life in the Digital Age?: Opportunities and Risks of the Digital Transformation for People's Well-being, https://doi.org/10.1787/9789264311800-en

SECTION 2

Current Regulations on Responsible Use and Identity in the Metaverse

Overview of Current State of Regulations

As the metaverse continues to evolve and gain traction as a digital realm for human interaction, it is imperative for organisations and individuals to consider the regulatory landscape surrounding responsible usage and identity management. However, there are a multitude of rules, laws and regulations that apply in a fragmented manner across the various activities the metaverse will be associated with. Additionally, current laws and regulations related to the protection of user-generated content, identity verification, and legal enforceability in physical jurisdictions do not fully account for the complexities of the metaverse, resulting in gaps and challenges for organisations operating in this virtual realm. There are questions on (1) which laws apply (existing or newer ones), (2) what is the cost of detangling the complexity and (3) how well will it serve the purpose for which it was designed. For the purposes of this policy paper, we are only addressing the critical legal issues posed by the existing regulatory landscape.

Most of the existing initiatives aim to address a number of key areas of priority in the metaverse, including:

- **Data protection**: The initiatives aim to provide a framework for the protection of personal data in the metaverse, including the use of avatars and virtual assets.
- **Copyright and IP**: The initiatives aim to provide a framework for the protection of user-generated content in the metaverse, including the use of virtual assets and the potential for infringement in real-time virtual environments.
- **Digital identities**: The initiatives aim to establish a framework for secure and reliable digital identities in the metaverse, including the use of avatars and the associated ownership of virtual assets.
- **Legal enforceability**: The initiatives aim to provide a framework for the legal enforceability of metaverse commitments in physical jurisdictions, including the resolution of disputes.
- **Internet Governance**: The initiatives include testing if the existing frameworks and regulations in respect of the Web can be extended to the metaverse.

It is worth noting that all these initiatives in the context of the metaverse and Web 3.0 are still in the early stages of development and implementation, and they may evolve and adapt as the metaverse and its ecosystem continue to develop.

Data Protection: Protection of personal data is a key problem as data fuels the metaverse. Data protection laws such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) that have extra-territorial scope need to be considered when handling user data. Laws such as the GDPR impose rules around data exportation and data localisation which in the metaverse becomes difficult to comply as there are layers of suppliers that result in various data transfers across the globe. Moreover, the existing data protection laws do not fully address the unique features of the metaverse, such as the use of avatars and virtual assets, and creates challenges for organisations in terms of obtaining informed consent and ensuring compliance with data protection regulations. The Organisation for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data provides a framework for the protection of personal data in the digital realm. The European Union's Digital Single Market (DSM) strategy aims to create a single market for digital goods and services in the EU. This strategy includes initiatives related to data protection, copyright, and digital identities.

Copyright and IP: The protection of user-generated content is a vital aspect of responsible usage, and legislations such as the United States' Digital Millennium Copyright Act (DMCA) and the European Union's Copyright Directive provide a framework for the protection of copyright holder rights and the removal of infringing content. E-commerce activities within the metaverse would be subject to laws, such as the EU Regulation on Promoting Fairness and Transparency for Business Users of Online Intermediation Services (Regulation (EU) 2018/0112), known as the "Platform to Business Regulation" (P2B Regulation).

Another challenge related to responsible use in the metaverse is the protection of user-generated content. While the United States' Digital Millennium Copyright Act and the European Union's Copyright Directive provide a framework for the protection of copyright in the digital realm, they do not fully account for the unique features of the metaverse, such as the use of virtual assets and the potential

for real-time infringement. This poses challenges for copyright holders and organisations operating in the metaverse.

Digital Identities: The use of virtual identities raises questions about the veracity and reliability of the information provided by users, identity authentication as well as the potential for anonymity and fraud. The National Strategy for Trusted Identities in Cyberspace (NSTIC) in the United States and the EU's Electronic Identification and Trust Services (eIDAS) regulation provide a framework for secure and reliable digital identities but they do not take into account the unique features of the metaverse, presenting challenges for organisations in terms of verifying the identities of their users.

Identity verification in the metaverse is another area where current laws and regulations are not fully equipped to address the complexities of the virtual realm.

Legal Enforceability: The legal enforceability of metaverse commitments in physical jurisdictions is an area of concern particularly when identification may be difficult and the participants may be interacting in real time but be physically present in another country. The metaverse is a global, decentralised environment, and it is not clear how the laws and regulations of different jurisdictions will apply and be enforced in the case of virtual transactions and disputes, which poses challenges for organisations in terms of ensuring compliance with legal requirements and resolving disputes.

Internet Governance: The Internet Governance Forum (IGF) aims to provide a forum for dialogue on public policy issues related to the internet. For example, discussions and forums have been held through multi-stakeholder dialogue on the metaverse. It is also worth noting the National Data Committee, MSIT, South Korea has stated that they will not make the mistake of regulating a new service (metaverse) with existing law. Hence there is a need to overcome the fragmentation of policies, standards, and frameworks at national and industry levels and consolidate the same into a coherent global framework that is understandable and easy to implement.

Other metaverse specific governance initiatives have been taken by South Korea and UAE. In July 2022, Dubai announced its Metaverse Strategy – its priorities included regulation refinement. South Korea has enacted the 3-year Metaverse Industry Promotion Act in September 2022 led by the metaverse policy review committee headed by the Prime Minister.

In November 2022, South Korea's Ministry of Science and ICT released eight core ethics principles (authenticity, autonomy, reciprocity, respect for privacy, fairness, personal information protection, inclusiveness, and responsibility for the future) which centre around three core values (sincere identity, safe experience, and sustainable prosperity) with the intent of providing a code of conduct for metaverse users and operators to align their actions.

While South Korea was the first country with a published framework focusing on the metaverse, it may be argued that many of the AI frameworks also apply to the metaverse. For example, Canada was the first country to launch an AI strategy in 2017[9] with calls for Responsible AI policy briefs. Its Responsible Use Of Artificial Intelligence (AI) Guiding Principles[10] for government officials may be extended with amendments to the metaverse. It is worth noting that according to WEF over 90 sets of 200 similar AI principles exist.[11] In the meanwhile, the EU aims to be the first major regulator to issue a unified regulation on AI, i.e., the AI Act. However, in contrast to the EU's approach, the UK has decided not to legislate to create a singular entity to govern the regulation of AI, and has instead elected to adopt to 'an adaptable approach to regulating AI' that supports existing regulators by identifying cross-sectoral AI principles that may be implemented by the regulators to suit their respective sectors.[12]

9 Canada's Artificial Intelligence Strategy https://cifar.ca/ai
10 Responsible Use of AI Guidelines https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai.html
11 World Economic Forum, 2022, 9 ethical AI principles for organizations to follow.
12 European Parliament (2023), EU AI Act: first regulation on artificial intelligence https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

SECTION 3

Key Metaverse Applications Developed Across Key Industries

A

Manufacturing
Healthcare
Tourism
Retail and Creative Economy
Education
Financial Services

B

Seoul
Barbados
China
Singapore
United Kingdom

A Overview of Key Metaverse Applications Impacting Key Industries and Sectors

While the gaming industry still drives the metaverse at this point of time. We are seeing a convergence of players and industries that make the metaverse exciting in terms of opportunities.

(i) Manufacturing

Manufacturing is approximately 16% of global GDP.[13] In manufacturing, the metaverse has seen the adoption of digital twins. However, this can be taken further where remote operations are needed, for monitoring, surveillance and even maintenance. Some exciting developments have been taking place in this sector. Hyundai Motor is planning with Unity (known for its 3D games) to deliver a Meta-Factory, which can create a digital replica of a physical factory supported by a metaverse platform. Korea Advanced Institute of Science & Technology (KAIST) introduced a virtual plastic screw factory for users to experience a simulated manufacturing environment with VR headsets. This virtual offering allows operators to alter factory settings without closing the entire factory, which would be required in the real world. JetBlue, an American airline corporation, engaged Strivr, a host of virtual reality environments, to provide VR training for its technicians in a simulated airplane environment. Besides the metaverse as a platform, the manufacturing of hardware for the metaverse and its infrastructure is likely to significantly increase. However, the adverse impact of such rapid automation and efficiency will be job loss and secondary effects such as higher cost of re-training, employment insurance and unemployment benefits. These trade-offs will need to be carefully examined at a global level. Moreover, in the space of metaverse digital twins, there are a few strong players emerging who are consolidating this sector which may lead to growing anti-trust issues.

(ii) Healthcare

The healthcare industry contributes 10% to the global GDP[14] and the lack of access to healthcare reduced global economy by 15%.[15] Metaverse technology has the potential to increase the contribution of the healthcare sector by offering services across borders to ensure timely interventions. While initially it could be for tele-health, diagnosis and consultation with experts, offering of therapies for mental health, in future, it could include remote surgeries. In this regard, it is worth referencing the DaVinci Surgical Robot which utilises VR/AR for conducting surgeries remotely.

The first Microsoft HoloLens orthopedic surgery in Latin America took place in 2020 by which the surgeon was able to view patient records via AR. In 2022, Thumbay Group and Medcare Hospitals (UAE) launched plans for a metaverse hospital. The challenge of managing the requirements of data laws like the Health Insurance Portability and Accountability Act (HIPAA) and yet providing exceptional personalised care is one that is something regulators need to consider. Yet, the use of digital twins or synthetic data may mean it is possible to test new drugs, therapies or surgeries before real intervention. In terms of health sandboxing, only few places like Singapore, India, Denmark and the State of Massachusetts have programs set up, yet more would be needed.

(iii) Tourism

Tourism contributes over 10% to the global economy and 1 in 4 jobs.[16] The tourism industry encompasses a wide variety of businesses and organisations that provide goods and services such as accommodation, transportation, entertainment, food and beverage, and other tourist-related services. To attract tourists, the industry employs various promotional strategies, including government initiatives, tourism boards, travel agencies, as well as word-of-mouth and social media marketing.

The metaverse will unleash entrepreneurship and travel even when borders are difficult to cross. By providing completely new ways to experience tourist

13 World Economic Forum, (2021), 9 ethical AI principles for organizations to follow.
14 WHO (2020), Global spending on health: Weathering the storm, https://www.who.int/publications/i/item/9789240017788
15 McKinsey & Company (2020), Prioritizing health: A prescription for prosperity, https://www.mckinsey.com/industries/healthcare/our-insights/prioritizing-health-a-prescription-for-prosperity
16 WTTC (2023), Economic Impact Reports, https://wttc.org/research/economic-impact

attractions it will increase revenue from this sector. For example, the creation of virtual replicas of real-world landmarks, sensitive archaeological sites and attractions could be used to attract tourists who may not visit (example elderly), or hold concerts without damaging historic landmarks, or to provide video game simulations (which will increase soft power of nations). Helsinki, Finland created a 3D Helsinki in Minecraft that not only had the city but neighbouring islands represented.[17]

Additionally, the metaverse can allow virtual tourists to visit museums, attend concerts, interactive comedy shows, and other tourist attractions in real-time alongside physical tourists through the use of digital twins. The Dubai World Expo 2020 held in 2021-22 attracted more virtual visitors than real visitors due to the pandemic. It can also create new experiences such as open-air museums where visitors can compare and contrast history and modernity through augmented reality. Furthermore, visitors can turn their unique experiences into non-fungible tokens (NFTs) and keep them as mementos of their touristic accomplishments. More importantly, one is able to preserve history, showcase culture, and also use metaverse experiences to teach geography or history. The challenge is whose history, whose culture and whose stories one will use to showcase places. This is a fluid area for future metaverse discussions.

(iv) Retail and Creative Economy

The retail sector accounts for 9% of global GDP and an additional 20% indirectly.[18] The metaverse will augment this sector through micro-transactions, decentralised marketplaces and virtual store fronts. This economic opportunity is expected to touch US$ 1 trillion.[19] The growth of NFTs, shopping for avatars and virtual real-estate are some examples of the possibilities of this platform. Retailers are looking at creating a virtual presence and curating experiences for loyal customers. Etisalat, a UAE telecommunications company, aims to replicate the design of their Dubai Mall store into a virtual environment. Brands are wooing customers through gaming platforms and pushing sales to brick and motar stores, working on CSR and creating word of mouth.

In addition to enhancing the shopping experience, the metaverse also has the potential to improve the efficiency and ethicality of the retail industry. By utilising virtual inventory systems, tracking sourcing, consumption and disposal, there may be greater opportunities to contribute to the circular economy and manage inventories to reduce loss. The additional challenge will be the immense amount of data being produced and the need for privacy with customised experiences. Further, the issue of copyrights and IP will get more complicated in a creator retail economy as the recent Hermès vs. MetaBirkins lawsuit shows.[20]

The creative industry contributes 3% of total merchandise exports,[21] 21% of total services exports, and 3% to world GDP.[22] The metaverse is driven by the creative industry. Gaming was an early fore-runner, and has technologically advanced in terms of embodied experiences. This sector also includes entertainment, arts, culture, publishing, and fashion. Half the jobs in this industry are accounted by women.[23] Most of the current fashion-related metaverse applications are focused on raising brand awareness rather than activities that generate direct income. However, this is expected to change rapidly – Morgan Stanley has predicted that digital fashion could increase the industry's sales by US$50 billion by the year 2030.[24] NFTs was one example where the creative industry found another method for expression and income generation. The challenge with the metaverse will be copyright infringement. The recent lawsuit by Getty Images on Stable Diffusion is one example of potential claims. The line between inspiration and copying will get harder to define in this new world.

17 HRI (2022), 3D models of Helsinki - Minecraft Helsinki3D+, https://hri.fi/data/en_GB/dataset/helsingin-3d-kaupunkimalli/resource/9e0d34a8-b0ed-46a0-889a-dadf40299406
18 IFC (2023), IFC›s Priorities in Retail, https://www.ifc.org/wps/wcm/connect/industry_ext_content/ifc_external_corporate_site/trp/retail/trp_priorities_retail
19 JP Morgan (2022). Opportunities in the Metaverse. https://www.jpmorgan.com/content/dam/jpm/treasury-services/documents/opportunities-in-the-metaverse.pdf
20 The New Yprk Times (2023), Hermès Wins MetaBirkins Lawsuit; Jurors Not Convinced NFTs Are Art, https://www.nytimes.com/2023/02/08/arts/hermes-metabirkins-lawsuit-verdict.html
21 UNCTAD (2022), Creative economy offers countries path to development, says new UNCTAD report, https://unctad.org/news/creative-economy-offers-countries-path-development-says-new-unctad-report
22 UNESDOC (2021), Cultural and creative industries in the face of COVID-19: an economic impact outlook, https://unesdoc.unesco.org/ark:/48223/pf0000377863
23 UNESCO (2021). International Year of Creative Economy for Sustainable Development, https://en.unesco.org/commemorations/international-years/creativeeconomy2021
24 Bernard Marr (2021), How Luxury Brands Are Making Money In The Metaverse, https://www.forbes.com/sites/bernardmarr/2022/01/19/how-luxury-brands-are-making-money-in-the-metaverse/?sh=5a78cd0b5714

(v) Education

Government expenditure on education is about 4.3% of GDP.[25] A report by Korn Ferry suggests that US$1 invested in workforce, results in US$11.39, more than tech or physical assets investments.[26] The first adopters in metaverse education are the health and engineering sectors. The COVID pandemic further encouraged experimentation in this sector. The metaverse offers an excellent opportunity for life-long learning, continuous education, skills development and formal education. Workplaces are using the metaverse for employees. Novartis, a pharmaceutical company trains lab employees on labelling; Walmart, a retailer trains employees for customer service; and Verizon, a telecom provider trains staff for safety scenarios.[27] Emirates Airlines is already planning to train future cabin crew in the metaverse, simulating the aircraft. In some cases they are interacting with simulations of people, and in other cases an avatar of an instructor.

The metaverse can be used to supplement in-class instruction by providing students with additional resources and activities that they can access outside of class allowing students to reinforce concepts and skills learnt in the classroom. In online learning, there are more partnerships emerging (for example City University of New York (CUNY), with the New York Jobs CEO Council to launch the EverUp Micro-Credential Program)[28] and this will also extend to the metaverse. This type of matching is needed to manage the skills shortage employers complain about.[29]

One challenge in this new industry is finding approved content and verifying the IP of the content – here the gap is four years between deployment of the app or experience and the research behind it.[30] Since formal education often involves minors, the challenge remains governance and to what extent do we want to gamify learning when the objective is self-learning or instead should it offer different pathways for learning to ensure no child is left behind?[31] Ministries of Education across the world have much work to do as they will be responsible to vet content and monitor the effects of experiential learning. The metaverse-based smart education ecosystem needs to be student-centered and yet dynamic, secure, and ensure that other key stakeholders like educators, psychologists, sociologists, learning and health specialists and employers are involved.

There has been a lot of activity in this space. In June 2022, the All India Council for Technical Education (AICTE), became the first accreditation agency office in the metaverse.[32] As part of the South Korean's Digital New Deal 2.0 initiative, nurturing talent and "providing people with opportunities to access metaverse without regional restrictions, and to participate in a variety of metaverse events," is an important part of the strategy.[33]

(vi) Financial services

While services supporting the metaverse such as legal, marketing, cybersecurity, content management and consultancy are all important, one sector that will grow is the financial and banking sector. Currently, the sector's development in the metaverse is in the nascent stage. If metaverse and Web 3.0 will move towards decentralisation on, there will also be more digital assets or tokens used to fuel the metaverse economy. This would be an opportunity for banks, who are normally far more conservative.

HSBC set up its first-ever virtual storefront on The Sandbox. JP Morgan opened a lounge in Decentraland. Earlier in the year, in their white paper, JP Morgan highlighted that US$ 54 billion is spent on buying virtual goods, more than on music.[34] While there are many fintech sandboxes, the metaverse will challenge the existing national sandbox or reglab as it is decentralised. The exchange rates of NFTs, tokens, cryptocurrencies with fiat are not very transparent and without a clear visibility on movement, may pose other risks like a shadow economy, and crime.

25 World Bank (2022), Government expenditure on education (% of GDP), https://data.worldbank.org/indicator/SE.XPD.TOTL.GD.ZS
26 KornFerry (2016), Korn Ferry Economic Analysis: Human Capital Nearly 2.5 Times More Valuable to Economy Than Physical Assets Such as Technology, Real Estate & Inventory, https://www.kornferry.com/about-us/press/korn-ferry-economic-analysis-human-capital-nearly-2-5-times-more-valuable-to-global-economy-than-physical-assets-such-as-technology-real-estate-and-inventory
27 World Bank (2022), Online Learning Campus, https://olc.worldbank.org/about-olc/education-meets-the-metaverse-reimagining-the-future-of-learning
28 McKinsey & Company (2022), Demand for online education is growing. Are providers ready? https://www.mckinsey.com/industries/education/our-insights/demand-for-online-education-is-growing-are-providers-ready
29 World Economic Forum (2022), These are the world›s most in-demand professions, https://www.weforum.org/agenda/2022/05/most-in-demand-professions-list-2022/
30 Brookings (2022), A whole new world: Education meets the metaverse, https://www.brookings.edu/research/a-whole-new-world-education-meets-the-metaverse/
31 Ibid.
32 Business Today (2022), AICTE gets office in the metaverse, https://www.businesstoday.in/crypto/story/aicte-gets-office-in-the-metaverse-336627-2022-06-07
33 MSIT (2022), MSIT to announce pan-government strategy on metaverse, https://www.msit.go.kr/eng/bbs/view.do;jsessionid=vYBYhaiMhA5Zylm7Gj86CxYlKbtD-jGrYq2lBdqZ6.AP_msit_2?sCode=eng&mPid=2&mId=4&bbsSeqNo=42&nttSeqNo=621
34 JP Morgan (2022), Opportunities in the Metaverse, https://www.jpmorgan.com/content/dam/jpm/treasury-services/documents/opportunities-in-the-metaverse.pdf

B

Overview of the Potential for Governments to Integrate the Metaverse within their Services (including the Current Initiatives in this Area).

A number of government agencies have began establishing their virtual presence in the metaverse (such as United Arab Emirates, South Korea, Barbados, China, Singapore and Norway). In November 2021, Decentraland and the Barbadian Ministry of Foreign Affairs and Foreign Trade signed an agreement to build a digital embassy on the Decentraland platform. In May 2022, Dubai's Virtual Assets Regulatory Authority[35] became the first regulator to establish its metaverse headquarters on The Sandbox platform. Meanwhile, in Shanghai, the local government of Fengxian and digital entertainment company Fengyuzhu are collaborating on a project to construct a virtual city hall that will replicate a real performing center in the Fengxian district. These initiatives indicate the significant potential for governments to integrate the metaverse into public services. An overview of the various government driven metaverse initiatives are set out below –

Korea

Seoul is one of the major cities that has integrated the metaverse into their provision of public services in various sectors. In November 2021, the Seoul government released the "Seoul Vision 2030" development blueprint and decided to invest 3.9 billion KRW in the development of the "Metaverse Seoul Basic Plan", which will provide the city with public services in the metaverse.

The government will build a virtual municipal government service platform of "Metaverse Seoul" to provide virtual services in seven areas, namely economy, tourism, education, communication, city development, administration and infrastructure.

In terms of public offices, the government plans to open "Metaverse 120 Centre", a virtual public service centre, in 2023. Citizens may meet avatars of public officials, resolve their civil complaints and benefit from consultancy services without physically being present at the Seoul City Hall. The government will also set up a metaverse mayor's office which will be used as an open communication and opinion gathering channel between the city and its residents.

Apart from government offices, the platform will allow citizens to create their own space and content, and host events such as exhibitions and marketplaces. It will also provide residents with a place for public gatherings so that they can congregate and spend time together.

For the education sector, a virtual campus of Seoul Open City University will be built to offer diverse immersive content, such as lectures, mentorship programmes, and careers fairs, to adolescents in the metaverse environment.

For tourism, major tourist attractions in Seoul (e.g. Gwanghwamun Square, Deoksugung Palace, and Namdaemun Market) will be created as "virtual tourism special zones", and lost historical resources (e.g. Donuimun Gate) will be reproduced in metaverse. The government is also seeking to hold Seoul's leading festivals (e.g. the Seoul Lantern Festival) in the metaverse so that people around the world can enjoy the festival.

Barbados

The Government of Barbados has also integrated the metaverse into their operational activities. The Barbadian Ministry of Foreign Affairs and Foreign Trade signed an agreement with Decentraland to build a digital embassy on Decentraland's platform in November 2021. They are currently finalising agreements with Somnium Space, SuperWorld and other Metaverse platforms. It is expected that they will set up more embassies in the metaverse on other platforms in the future. According to the 1961 Vienna Convention (Article 1 (i)), embassies have traditionally been physical spaces hence navigating this new space for diplomatic relations will need to be acknowledged.

35 https://www.vara.ae/en/f

China

The Chinese government is seeking to integrate the metaverse into public services. The December 2021 Shanghai Municipal Commission of Economy and Information Technology's five-year development plan for the electronic information industry listed four frontiers for exploration, one of which is the metaverse. While the plan did not specify a timeline for metaverse research and development, it does call for "encouraging the application of the metaverse in areas such as public services, business offices, social entertainment, industrial manufacturing, production safety and electronic games", which indicates the Chinese government's interest to integrate metaverse into its public services.

Notably, a government project in Shanghai (a collaboration between the local government of Fengxian, a new suburban district under construction, and Fengyuzhu, a Shanghai-based digital entertainment company) has already been launched. The government will build a virtual city hall, which will be a virtual replica of a real performing centre in the Fengxian district "to let local residents and tourists feel the urban development progress" and it will potentially become a government services portal.

Singapore

While there are no immediate official plans to integrate the metaverse into public services, government officials have started to explore the possibility of integrating the metaverse into their public services. According to Singapore's Second Minister for Law, Edwin Tong, legal services such as marriage proceedings, court case disputes, and government services could be offered in the metaverse and he envisions that the metaverse could be integrated into their dispute resolution practice. In this context, Decentraland has hosted its first marriage ceremony in its metaverse virtual world in 2022. Although the union may not be legally recognised by law, there is certainly a potential that governments will try to integrate the metaverse into public legal services.

United Arab Emirates

The Dubai Metaverse Strategy launched in 2022 aims to turn Dubai into one the world's top 10 metaverse economies as well as a global hub for the metaverse community. The strategy aims to build on Dubai's achievement of attracting more than 1,000 companies in the fields of blockchain and metaverse. It also promotes Dubai's ambitions to support more than 40,000 virtual jobs by 2030. In consonance with this strategy, in 2022, Dubai's Virtual Assets Regulatory Authority became the first regulator to establish its metaverse headquarters on The Sandbox, and hosted the Dubai Metaverse Assembly where more than 300 global experts, policymakers, thought leaders, and decision-makers from over 40 organisations met to identify the best ways to leverage metaverse centric opportunities across strategic sectors of countries, governments, and companies. Other significant government driven initiatives include its Ministry of Health and Prevention's 3D Digital Metaverse Assessment Service and

Metaverse Customer Happiness Service Centre. The former enables remote evaluation of healthcare practitioners. The 3D platform simulates a realistic assessment with defined roles and platforms for the judging committee, invigilators, and examinees. The latter established the world's first customer happiness service centre at the Arab Health 2022. Another noteworthy initiative is the UAE Federal Authority for Government Human Resources (FAHR)'s use of the digital platform Jahiz to provide government employees training on AI and metaverse technologies.

United Kingdom

The UK's National Digital Twin Programme (NDTP) acts as a focal point to grow national capability in digital twinning, as set out in the Integrated Review 2021. It is undertaking work to understand the need for, and develop, the standards, frameworks, guidance, processes and tools that will:

- enable people to gather, process, manage, store and share information in a way that ensures the right information is available at the right time, to the right people and that the quality of the information is understood; and

- enable users to engage with, visualise and analyse the information in a way that meets their needs and allows them to optimise decision-making.

As we can observe from above, there are many industry specific initiatives focusing on public value encouraged by governments. This is an evolving space and dialogue should be facilitated in order to develop common frameworks across sectors and nations.

SECTION 4

Key Areas of Priorities

(i) Online and Transboundary Harm and Crime Prevention
(ii) Data Protection and Privacy
(iii) Sovereignty & Cybersecurity
(vi) Digital Well-being and Addiction
(v) Protection of IP
(vi) Sustainability

(i) Online and Transboundary Harm and Crime Prevention

The metaverse will not only result in online harm but harms that cross over to the real world. While the laws for the real world are well-defined (though there are loopholes and/or grey areas of interpretation), for transboundary and cross-jurisdiction harm and crimes, the area is grey.

Online harm may occur at individual, societal, industrial, national, global or regional , and trans-generational levels.

For example, at an individual level, it can be against a person (mentally and physically, or their virtual representation and virtual property). Specifically, we find a dearth of laws on the protection of minors though they exist at some industry level. At a societal level, the harm could be cultural appropriation or stereotyping, which could create online bias against a whole set of the population. At an industry level, the metaverse could lead to massive onboarding of technologies that are not inclusive or the appropriation of technology/IP that reduces future competition (especially in a world where the user is the co-creator). Finally, at the national level, online harm could lead to attacks on national sovereignty (this will be covered separately under section Section 4(iii).

There are some laws and regulations in place across countries for these issues. The challenges are documenting cross-over crimes, the tension between cyber-surveillance/security versus privacy, and monitoring trans-generational harm. Many laws that currently exist also cover crimes in the metaverse, like that of identity theft – the US' 1998 Identity Theft and Assumption Deterrence Act; or India's IT Act 2000 and Amendment to the IT Act via section 66-C. However, there are still grey areas on liabilities from harm. Specifically, this section will look at the protection of minors and societal harms (including to minority and vulnerable groups).

(a) Protection of Minors: This is an evolving space. At the end of 2022, Epic Games Inc., the maker of games like Fortnite (with investments from Sony and Tencent Holding) was fined US$520 million by the US Federal Trade Commission (FTC). This fine was for violating the Children's Online Privacy Protection Act (COPPA) by collecting information about children under the age of 13 without parental consent and using "dark patterns" to trick them into unwanted purchases. These spaces (data collection and gamification for micro-purchases) have always been a grey area. Games like these are rated for teens, but it is obvious that younger children play such games. The company, while acknowledging the settlement, highlighted the challenges of governance in this space: "The video game industry is a place of fast-moving innovation, where player expectations are high and new ideas are paramount. Statutes written decades ago don't specify how gaming ecosystems should operate. The laws have not changed, but their application has evolved, and long-standing industry practices are no longer enough. We accepted this agreement because we want Epic to be at the forefront of consumer protection and provide the best experience for our players." In response,[36] the company introduced significant changes: more parental oversight, a daily spending limit for children under 13, and a default setting for the highest privacy level for minors under 18. The industry needs to share common practices of high standards so that the design and deployment of metaverse worlds have inbuilt default protection for minors.

COPPA (US), enacted in 1998, became effective in 2000, and was amended in 2013. It focuses on websites and online services. UK's Online Safety Bill (2022) will put more responsibility for user safety on providers. For example, for social media, children under 13 are not allowed, and providers must use age assurance or age verification technologies.[37]

36 Statement from Epic Games dated 19 December, 2022: https://www.epicgames.com/site/en-US/news/epic-ftc-settlement-and-moving-beyond-long-standing-industry-practices

37 There have been significant developments around age assurance technologies in recent times. The German regulator KJM has reviewed and approved over 100 methods of age assurance in the last decade. Under the Digital Regulation Co-operation Forum (DRCF), Ofcom and the ICO jointly commissioned research to explore ways of measuring the accuracy levels achievable by different age assurance solutions (https://www.drcf.org.uk/publications/papers/measurement-of-age-assurance-technologies). The French data protection regulator, the CNIL, has stated that "it considers acceptable the use of age verification by validation of a payment card or a process of facial age estimation based on facial analysis without facial recognition". In 2018, the PAS 1296:2018 Online age checking was issued. There are also the IEEE and ISO standards which are currently going through the standards development process, the first of which is due to complete in the coming months.

In the case of online harm, the duties of a parent or caretaker, or even online service providers are implied.[38] The Office of Communications (Ofcom) will be responsible for compliance with fines of up to £18 million or 10 percent of their annual global turnover, and with the possibility of prosecution of senior managers who fail to comply with Ofcom requests. Moreover, the UK Information Commissioner's Office has also published an 'Age appropriate design: a code of practice for online services' (also known as Children's Code) to help protect children in the digital world and aimed at online services, such as apps, gaming platforms and web and social media sites, that are likely to be accessed by children. In the United Arab Emirates, the Digital Well-being Council is a government council established in 2018 with the aim of promoting digital well-being among residents. The council focuses on addressing issues related to excessive use of technology and the potential negative impacts on mental and physical health, relationships, and productivity. It collaborates with various government entities, private organisations, and experts in the field to develop strategies and initiatives to promote healthy technology use and improve digital well-being for all individuals in the UAE.

Other high-level guidelines are OECD's Recommendation of the Council on Children in the Digital Environment (which includes critical stakeholders in the metaverse such as content providers, ISPs, and hardware manufacturers); ITU's published guidelines on child protection online, and The Council of Europe's Strategy for the rights of the Child (2022 – 2027).

When parents do not embrace the new technologies, there is a gap in societal education that must be filled quickly as online services on the metaverse will be device agnostic with increasingly easier access.

(b) Societal Harm: While the UK Online Safety Bill (2022) covers adults, society, and national sovereignty, more work is required internationally. One challenge is identifying whose responsibility it is for safeguarding against harm. For example, Canada's Personal Information Protection and Electronic Documents Act ('PIPEDA') puts the obligation on the service provider. This suggests that companies operating in the metaverse (where co-creation may be the norm) will have to increase content moderation, cybersecurity and plan for higher insurance costs. This also implies smaller companies may not be able to manage their operating costs, which may affect industry competitiveness.

The challenge for nations is determining the applicable jurisdiction as metaverse crimes are typically online and borderless thereby making prosecution hard. While in some cases, the prosecution may occur with "extraterritorial jurisdiction," often this happens for geographic crimes (not yet online). There is a discussion on the extra-territorial application if components of global AI systems are used, developed, designed, or managed in the country/region (for example, data transfer/sovereignty). Some new acts have emerged in this space: EU Digital Markets Act, EU Data Act, EU AI Act, and the Canada Digital Charter Implementation Act 2022 (bill introduced).

In Australia, the eSafety Commissioner has powers under the Online Safety Act 2021 (Cth) to make sure that services and devices, including those enabling access to metaverse environments, are as safe as possible. The eSafety Commissioner can investigate and take action to address complaints from individuals experiencing specific types of online harm, including cyberbullying. In addition, the eSafety Commissioner is empowered to regulate systems and processes through a broad set of Basic Online Safety Expectations as well as enforceable, co-regulatory industry codes or standards dealing with content such as child sexual exploitation material and terrorist and violent extremist material.[39] The eSafety Commissioner has also developed a voluntary framework for Safety by Design, which provides the online industry with guidance on how to incorporate online safety into their digital products and services. The framework includes three principles: Service provider responsibility, User empowerment and autonomy and Transparency and accountability.[40] By adopting these principles, organisations can create safer digital experiences for users and mitigate potential harm from online risks.

38 FTC says in its FAQ 11 "COPPA is meant to give parents control over the online collection, use, or disclosure of personal information from children. It was not designed to protect children from viewing particular types of content wherever they might go online. If you are concerned about your children seeing inappropriate materials online, you may want to consider a filtering program or an Internet Service Provider that offers tools to help screen out or restrict access to such material." FAQ 12: COPPA covers operators of general audience websites or online services only where such operators have actual knowledge that a child under age 13 is the person providing personal information. The Rule does not require operators to ask the age of visitors. However, an operator of a general audience site or service that chooses to screen its users for age in a neutral fashion may rely on the age information its users enter, even if that age information is not accurate. In some circumstances, this may mean that children are able to register on a site or service in violation of the operator's Terms of Service. If, however, the operator later determines that a particular user is a child under age 13, COPPA's notice and parental consent requirements will be triggered. Available here: https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions

39 https://www.esafety.gov.au/industry

Many of these new regulations work on the classification of service providers (the challenge is that they mostly focus on the service providers as opposed to other stakeholders) and have been defined in the context of AI (EU) or online safety (UK). The new UNESCO Guidelines for Regulating Digital Platforms (Draft 2.0) also outlines responsibilities of platforms.[41] This is an area that needs more clarity particularly where through the use of technology, the entities supplying or making the metaverse services available may be decentralised and may not be capable of supervision in the same manner as a traditional legal (centralised) entity.

In the meanwhile, there have been some global coalitions which have begun focusing on metaverse crimes: INTERPOL launched its Metaverse police in October 2022 although existing task forces like the INTERPOL Financial Crime and Anti-Corruption Centre launched in 2022 will focus on transnational financial crimes.

(ii) Data Protection and Privacy

Data privacy is a significant concern in the metaverse. A recent IBM study found that 81 percent of consumers say they have become more concerned with how their data is used online.[42] Moreover, given the vast volume of personal data processed by all kinds of technical applications and devices, the regulation of personal data is necessary to safeguard the privacy of the individual and the integrity of personal data. Currently, there is a lack of regulation in this space from a privacy perspective and the existing privacy regulations pose further questions on how this will be applied in the metaverse. Some of the key considerations from a privacy and data security perspective for operating in the metaverse include -

(a) Unprecedented volume and types of datasets processed

The metaverse is built on a large volume of data sets that will require significant personal data for customisation. Indeed the volume of data produced is anticipated to exponentially increase. It is estimated that 463 exabytes of data will be generated daily by 2025 vs. 1200 petabytes of data currently stored by Google, Meta, Microsoft and Amazon.[43] The unprecedented volume of personal information is exacerbated by various challenges in this area as highlighted below.

- We cannot separate the data collected via the avatar from the individual. Hence, any data collected in relation to an avatar, although in a different form from that of the individual, constitutes personal data. For example, registrations/sign-ups, payments, service interactions, system data generated via log-ins etc.

- Combining datasets collected from multiple sources including anything from gait, gaze, posture, emotion and haptic data involving sensations as well as interactions with other individuals, content and objects in real time, if they are ascribed to a single person may still constitute personal data.

- Even if anonymous or intentionally incorrectly reported, there is a potential that such data may even constitute special category or sensitive data under data protection laws requiring a higher degree of protection. For example, children's data.

(b) Data sharing amongst multiple stakeholders, platforms, devices etc. and the role of user's choice

- Interoperability between different devices, platforms, and environments where large amounts of personal data are shared between parties, raises concerns as to how to ensure data security and privacy.

- Users will be able to move around between different spaces of the metaverse so that multiple data sets can be collected or shared.

- Software developers and brands will need to establish bilateral or multilateral data sharing agreements to improve the seamlessness of the consumer experience.

(c) Data privacy and security in the metaverse

- Security risks occur in relation to the ownership and transactions of any digital assets, including NFTs and cryptocurrencies.

- Maintaining end-user identification is essential to prevent identity theft in the digital world, especially

40 https://www.esafety.gov.au/industry/safety-by-design
41 UNESCO (2023) Guidelines for Regulating Digital Platforms (Draft 2.0).
42 Chakravorti, B. (2020), Why companies make it so hard for users to control their own data. Harvard Business Review https://hbr.org/2020/01/why-companies-make-it-so-hard-for-users-to-control-their-data
43 Statistica (2022), Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2020, with forecasts from 2021 to 2025, https://www.statista.com/statistics/871513/worldwide-data-created/

considering the possibility to imitate an end-user's avatar during user-to-user communication. This is becoming more critical with the advancements of deep fake technologies.

- Due to its interoperability and interconnection, personal data stored within metaverse enabling devices are exchanged in real-time. Consequently, the security integrity of a single device cannot guarantee data protection when the personal data is being transferred to multiple enabling devices.

- Lack of proper technical and organisational measures to offer adequate protection of these devices increases the risk of breach of security, which may lead to accidental or unlawful loss or access to personal data of the metaverse end-users.

- Existing data protection regulations envisage prior informed user consent to processing of any personal data. However, in the metaverse, there may be impossibility of compliance with these regulations given that personal data may be created in real-time that could not have been anticipated at the time of obtaining user consent.

The regulatory landscape around data privacy and security has significantly evolved in recent years with legislations leaning towards granting consumers control over their personal data (for example, GDPR in the EU). However, complex issues on scope of applicability of existing data protection and privacy laws in the metaverse as well as enforcement arise. Regulation of a digital interaction may involve the engagement of privacy rules in some countries based on physical location of the organisation or the individual; the type of organisation or individual (for example, a health care provider or a child) or the type of data collected and the purpose for collecting the data (for example, marketing or profiling). Other complicated issues include cross-border data transfer restrictions and data localisation requirements under local laws that may need to be addressed in the metaverse. A 2021 study by ITIF found that 62 countries have bans or restrictions on cross-border data flows, and the pace of these restrictions are accelerating.[44] Another aspect critical to consider will be the allocation of liability in the event of a data breach or harm - for example will this be the platform operator, operator of service or individuals?

In view of the above challenges, there is a need to establish and adopt common responsible data management practices and principles throughout the data lifecycle to enable the safety and protection of indviduals' personal data. The Fair Information Practice Principles (FIPPs), the OECD's Guidelines, and other privacy standards and guidance tools can be leveraged for this purpose. Additionally, there is a need for for cross-border collaboration and standardisation, following deep examination of globally and nationally accepted regulatory best practices for data privacy, data protection, and data security.

(iii) Sovereignty and Cybersecurity

Protecting sovereignty overlaps with national cybersecurity strategies. Most countries have laws to protect national sovereignty but the monitoring and implementation are difficult, especially across jurisdictions. The EU consolidated individual member strategies under an umbrella framework Network and Information Security Directive (NIS Directive) in 2016 (proposed in 2013).[45] This could potentially be adapted and extended for the metaverse across more geographies.

The challenges with cybersecurity will escalate in the future. By 2025, cybercrimes will cost the world US$ 10.5 trillion each year (for perspective, in 2021, the global cost was $150 billion).[46] While national cyber-security strategies and global standards are in place (for example, W3C),[47] there is a need for more in terms of international cooperation. The UK National Cybersecurity Plan (2022)[48] also acknowledges the importance of partnerships. UK is in the process of establishing a new international multi-stakeholder cybercrime treaty which sits alongside the Budapest Convention.

In addition, there is a need to add cybersecurity skills to the digital skills education. For example, as part of the Estonia Cybersecurity Strategy, they conduct

44 How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them | ITIF
45 ENISA (2023), National Cybersecurity Strategies Guidelines & tools, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools
46 As cited in McKinsey & Company (2022) New survey reveals $2 trillion market opportunity for cybersecurity technology and service providers: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers
47 W3C – More: https://www.w3.org

a cyber battle for youth.[49] Further, they host the Cyber Coalition,[50] a NATO exercise that has taken place annually since 2008. The UAE's National Cyber Security hosts the annual Cyber Quest Competition aimed at promoting and enhancing cybersecurity skills among Emirati students. The competition involves various challenges and tasks to test participants' knowledge and skills in cybersecurity concepts, digital forensics, cryptography, and ethical hacking since 2015.[51] The Singapore Cybersecurity Strategy 2021 looks at pipeline talent and international cooperation as key to creating a healthy digital ecosystem.

The UK spends £22 billion on research and development for cybersecurity.[52] At a global level, massive amounts of investment are applied in research and development but there does not appear to be a coherent research strategy into key metaverse governance and security projects. This needs to change.

Digital trust will become important. For instance, Singapore has developed an "SG Cyber Safe Trustmark and Cyber Hygiene Mark." This needs to be extended to create a global metaverse cybersafe trust mark and to especially ensure even small players and startups can access these services.

(iv) Digital Well-being and Addiction

Well-being in the metaverse is difficult to measure because the metaverse traverses various aspects of daily life in the real world. There have been studies where too much online play can be a challenge. While compulsive gaming can be a psychiatric disorder, this is a grey area. In 2013, the American Psychiatric Association declared compulsive gaming as a diagnosable disorder, and in 2018, WHO recognised it as a disease. While game mechanics are creeping into other spheres (social media, education, and work), there is a caution. There are inadequate medical facilities that diagnose or treat health risks associated with digital platforms addiction or insurance/health coverage for the same.

Content is another area that can affect well-being, and though some standards exist like the Pan European Game Information (PEGI) and Entertainment Software Rating Board (ESRB), there continues to remain a need for more guidelines and standardisation across countries.

Increasingly, there has been more research focus on digital well-being of children: The EU Horizon 2020 call for 2023-2024 Staying Healthy (in an increasingly digital society) focuses on children and adolescents;[53] UNICEF with the LEGO Group, is leading the Responsible Innovation in Technology for Children (RITEC) initiative which explores what wellbeing for children looks like in the digital age. In 2019, China's Online Game Anti-Addiction System (OGAAS) got stricter, however there are loopholes.[54] Moreover, countries also appear to be unsure of this space. South Korea, for example, ended the Cinderella law (which limited the time children under 18 played online) as the whole world went online during the pandemic.

More research is also needed to look at well-being of adults in the digital space. Apart from health problems caused by exposure to light-intensive images and extended usage of the VR/AR devices, users may experience mental issues due to unpleasant events in the metaverse or even inability to distinguish virtual life from reality.

Younger users or users with pre-conditions may be particularly vulnerable to such mental health problems. According to research reports, immersive technology can project a powerful illusion of reality, overloading the senses and contributing to addiction. Users may even experience withdrawal symptoms after leaving the metaverse.

Accessibility is another critical aspect for the metaverse. Currently, there are barriers for

48 UK (2022), National Cybersecurity Plan, https://www.gov.uk/goverhttps://en.unesco.org/commemorations/international-years/creativeeconomy2021nment/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022

49 E-Estonia (2023), e-Estonia Programme for Cyber Security, https://e-estonia.com/programme/cyber-security/

50 NATO (2022), NATO's flagship cyber defence exercise kicks off in Estonia, https://www.nato.int/cps/en/natohq/news_209405.htm?selectedLocale=en#:~:text=-Cyber%20Coalition%20is%20a%20long,national%20capitals%20and%20other%20locations.

51 Cyber Quest Competition https://www.thenationalnews.com/business/technology/uae-schoolchilden-pit-wits-against-each-other-in-cyber-security-competition-1.132039

52 UK (2022), National Cyber Strategy 2022, https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022#foreword

53 EU Horizon 2020 calll for 2023-24 – Staying Healthy. Available:https://sciencebusiness.net/sites/default/files/inline-files/HORIZON-Cl1%2006_23_2022.pdf

54 The 2019 amendment to the 2007 law limits minors to less than 1.5 hours of online games on weekdays and three hours on weekends, with no game playing allowed between 10 p.m. to 8 a.m. It also limited how much minors could spend on virtual gaming items each month, with maximum amounts ranging from $28 to $57, depending on the age. In August 2021, this time was further reduced by requiring online game providers to offer only one-hour services to minors from 8 pm to 9 pm on Fridays, Saturdays and Sundays, as well as on official holidays. https://mygamez.com/resources/blog/china-s-new-online-game-anti-addiction-real-name-authentication-system/ However, the minors have switched to short video apps. https://www.globaltimes.cn/page/202211/1280323.shtml

accessibility for people of determination, those without access to the internet or are too old to learn new digital skills. There have been local legislative initiatives undertaken to address this issue however not enough globally. For example, Colorado passed a law requiring websites from state and local public entities to meet accessibility standards.

OECD 2019 report, "How's Life in the Digital Age: Opportunities and Risks of the Digital Transformation for People's Well Being," specifically states that digital opportunities and risks are not correlated across countries thereby making it very difficult to create policy frameworks.[55] Digital skills are critical for resilience and well-being. For example, the EU 2030 Digital Compass highlights that this is an area we lag when compared to onboarding new technologies. Governments worldwide need to do more in this space as it is difficult to predict future jobs and the associated skills.

(v) Protection of Intellectual Property

Currently, IP protection of patents, copyright, and trademarks fall under the World Trade Organization (WTO), but there are challenges. In a co-created metaverse economy, there are issues of ownership and credit that may need to be explored, particularly, given that the cost of enforcement for an individual may be too high. Further, reverse engineering code or decompilation is not always illegal. The regulations seeking transparency of codes create tension with competitiveness. Hence, governments need to manage the fine balance and build greater trust.

Another issue of IP may be digital legacy. Facebook allows you to nominate a legacy contact, Google has an 'inactivate account' option for deceased users, and Microsoft has an appointment of custodian option, to manage your account when contacted by your heir. These issues will get compounded in a Web 3.0 environment where perhaps the content may become valuable or monetisable. As of now, digital property is not easy to bequeath and often falls between data protection laws and succession laws (currently ignored).

Finally, another challenge where the metaverse will not mirror the real world is that it does not have the same scarcity issues (for example, real estate). Hence you could have several cities pop up resembling real-world cities. Should there be an authorised version of the city? Who would own it? Would an NFT alone be enough to validate and authenticate the image when the same city appears in multiple spaces? IP laws are not very clear on this.

Below we present three key issues of IP - ownership of IP, protection of IP and disclosure or transfer of IP.

(a) Ownership of IP rights in the metaverse:

Two key aspects of the metaverse are that it will be immersive and interactive. Both of these aspects are likely to have consequences for the creation of IP.

The immersive nature of the metaverse is likely to mean that there will be greater opportunities for users to create IP when participating in the metaverse than they have done when participating in Web 2.0 applications. This fact may alter the balance of power between metaverse service providers and participants/content creators on the issue of which party owns the IP created by the participants and what rights either party has to use/exploit the IP.

The interactive nature of the metaverse means that users may create new IP in a variety of ways, in some instances in combination with other participants/ content creators. Without agreement regarding how the content so created is owned and/or shared between the parties, this may result in the IP created being subject to "deadlock" as many jurisdictions do not allow for one co-owner to exploit IP without the consent of the other co-owner. This fact is likely to be addressed by the platform owners through application of terms and conditions which provide for how IP is distributed between the parties.

A further point for consideration is the possibility that avatars creating IP may be operated by internet bots or AI. The question as to whether material created by AI can be protected by IP rights has been the subject of widespread debate. Some countries have determined that AI created materials cannot attract IP protection. More widespread adoption of the metaverse will make this an increasingly important issue because of the higher volumes of such materials which will be created as metaverse adoption grows. Where materials have been created through a combination of AI and human participants, this is likely to result in complex questions as to whether IP arises in respect of the materials created and, if so, who owns such materials and in what proportion. Typically, these kinds of issues have

55 OECD (2019). How's Life in the Digital Age?: Opportunities and Risks of the Digital Transformation for People's Well-being How's Life in the Digital Age?

been resolved through complex factual enquiries (normally in the context of high profile copyright works which have attached income streams). The fluid nature of the metaverse is likely to make these factual enquiries more complex.

(b) Protection of IP rights related to the metaverse:

To drive the expansion of the metaverse, it will be important for brand owners and creators to be able to protect their IP rights in the metaverse. In most countries, IP laws are a mixture of pre-existing laws which have been revised or supplemented to take account of subsequent technological developments, notably the rise of the internet. Many of these supplemental changes have been made to future-proof IP law against further technological developments. One of the ways in which this has been done is to adopt "technology neutral" definitions, for example in relation to infringement.

(c) Disclosure regarding transfer of IP rights in the metaverse:

IP licensing is another key area where industry players face challenges. It is sometimes not clear in the metaverse as to what is purchased and what is sold. In the context of NFTs, purchasers may often misunderstand the rights they are acquiring. For example, a buyer may not understand that they are only acquiring an NFT as a digital asset and that they are not acquiring IP rights to the underlying work.

(vi) Sustainability

Sustainability is the interconnection of three elements — social connection, economic well-being, and a healthy environment. To be sustainable, the internet also needs to assess, mitigate, and live up to its responsibilities for a healthy environment - an element that is too often neglected.[56]

Sustainability is a layered notion. It begins with the individual - what services and products they consume. Hence, there is an awareness or education issue and right to information issue (which needs to be common and easy to understand). Some standards exist, for example, the EU Digital Rights and Principles, but there is no guidelines for an individual to base their purchase and consumption patterns using sustainability indicators.

At the industry level, there are many new frameworks emerging: 30x30 COP 26-27 (Very High Level) – protection of 30% of land and oceans for nature by 2030; WEF Internet of Things: Guidelines for Sustainability; IEEE Planet Positive 2030 (in progress); ISO 26000 (ISO 20400 Sustainable Procurement - Guidance); UK's Competition and Markets Authority (CMA) (2021) guidelines and the OECD 2020 guidelines. However, like AI Ethics frameworks, these may not be easy to implement.

For the metaverse, there is a need to look at supply chain and accountability. Data often travels around the world, and this increases its carbon footprint. Also, as the metaverse will merge with the IoTs, this may also be a challenge in terms of energy, resource consumption and recycling. Some recent initatives in this space could be the European Commission's "Supporting the Green Transition".

While there is some focus on sustainability via individual government regulations and other global initiatives, it is not enough, as the ability to measure the impact on SDGs is difficult. Neither are the initiatives and frameworks easy to translate for the metaverse, which is global and borderless.

(vii) Advertisement

The media and advertising industry has heavily involved itself in the digital world, with examples such as social media personalised ads and the use of AI and other technologies. However, the development of advertising will continue to grow as the metaverse continues to develop. Brands often change and evolve their advertising strategies to keep up with changing trends, due to fear of missing out and the low barriers of access to digital platforms. Additionally, brands will often extend their business across multiple channels and generate new revenue streams through virtual assets and services.

Accessing the metaverse has its advantages in reaching new demographics. For instance, it is difficult to reach gamers through traditional advertising. Therefore, brands have created new, authentic experiences tailored to gamers. Finally, brands can access the metaverse by engaging with the community through creating virtual assets and content.

56 Observer Research Foundation (2021), A sustainable internet: Missing pieces to a healthy future, https://www.orfonline.org/expert-speak/sustainable-internet-missing-pieces-healthy-future/

According to Media Monks,[57] brands are discussing how they can create "brand virtualisation" by adapting their brand exposure to new digital environments, relationships with stakeholders, and activities within the metaverse. The idea of virtualisation is to build a 3D presence that can help brands unlock new revenue streams. In recent years, there has been a lot of enthusiasm around NFTs and brands have taken advantage of this by branding virtual lands, objects, or sponsoring events in order to align with their mission or create further brand exposure. For example, Monster Drink collaborated with Tencent to place their logo on virtual assets in games, and Nike collaborated with Fortnite to create 'Fortnite Creative Mode' to enhance their brand exposure.

It is important for advertising agencies and brands to be aware of the role that the metaverse will play in the future. As we transition from community sharing to community participation, brands need to understand their role in co-creating digital experiences with the metaverse community.

Advertising Challenges

- **Digital Divide**: Not everyone in the world will have access to the immersive technologies or even the connectivity that these new experiences rely on, or even access to digital financing and payment.

- **Data Privacy**: Advertising companies will be targeting their clients via personalised content, which raises concerns about data privacy. Companies must ensure they are compliant with regulations and that they are transparent about how they collect and use consumer data.

- **Responsible Citizenship**: The ability to influence minds and norms should be underscored. Hence, there needs to be a responsibility towards global citizenship.

57 Media Monks (2023) The Metaverse Demystified. https://media.monks.com/articles/get-versed-metaverse

SECTION 5

Proposed Self-Regulatory Principles to Apply to the Metaverse

Interoperability for Access
Privacy by Design and Default
Sustainability by Design
Reciprocity
Transparency for Trust
Fairness, Equality and Inclusiveness
Commitment to Diversity
Accountability
Safety by Design and Beneficence

Nine Principles

Interoperability for Access	To allow users to be able to transport their data, digital assets and identities across platforms, regardless technical, jurisdictional or geographical barriers that may exist.
Privacy by Design and Default	To ensure that users' rights and personal data are protected and respected at each stage of the data lifecycle as the metaverse expands and operates.
Sustainability by Design	To ensure that sustainability (energy efficiency) is integrated into the design of the metaverse, right from the start.
Reciprocity	To promote trust and fairness by creating a culture where users and stakeholders are more likely to cooperate with each other, share resources and ideas, and work towards a common goal.
Transparency for Trust	To encourage the development of products and services that are designed with user experience and expectations in mind, and that are transparent about their workings, user rights, and data collection practices.
Fairness, Equality and Inclusiveness	To ensure that all individuals have an equal opportunity to operate in the metaverse and there are no barriers for their entry into the metaverse.
Commitment to Diversity	To ensure that the metaverse is inclusive and represents the diversity of the real world.
Accountability	To ensure responsibility and accountability for metaverse systems, technologies and their outcomes including being accountable for any harm.
Safety by Design and Beneficence	To ensure that users are protected from harm, and that the metaverse is a safe and positive space for everyone

The metaverse is an exciting new virtual world where users can interact with each other and digital objects using various technologies like advanced virtual reality and augmented reality. As this realm continues to grow and become more integrated into our daily lives, it is crucial to establish self-regulatory principles that prioritise the safety and well-being of all users.

One of the key benefits of implementing self-regulatory principles is building trust and credibility in the industry. By demonstrating a commitment to ethical practices and user protection, the metaverse can foster a sense of security and comfort for all participants.

In this paper, we will explore the non-exclusive self-regulatory principles that are essential for the metaverse. These principles cover a range of topics, including protecting user privacy, promoting ethical practices among developers and content creators, ensuring safety and security for all participants, and more.

By implementing these self-regulatory principles at a first step, we can commence the process to help ensure that the metaverse is a safe, enjoyable, and trustworthy space for all who participate in it.

Interoperability for Access

Interoperability is a key principle that is essential for the metaverse to reach its true potential. In simple terms, interoperability is the ability for users to move between the physical world and the various metaverse spaces, bringing their avatars, data, and digital assets with them. This means that users should be able to transport their digital assets and identities across platforms, regardless of the technical, jurisdictional or geographical barriers that may exist. Interoperability is significant because it increases usability, as users will not be locked into a single platform and can easily move between different metaverse environments. This also allows for greater communication and collaboration between all stakeholders (like providers, users, creators) as they will be able to easily share data and assets across different platforms and devices. Additionally, interoperability can lead to increased competition between platforms, as users will be able to easily compare and switch between multiple options.

Achieving interoperability is not a simple task and requires significant investment in platform architecture and operation. This includes the development of common standards and protocols, as well as the implementation of incentives to prompt firms to make these outlays. Some regulatory obligations for interoperability already exist, such as the right to data portability requirements within data protections (such as GDPR). Other frameworks like the Digital Markets Act (EU) mandate interoperability amongst the largest firms in the digital economy. When in force, it will require vertical interoperability between their hardware, software and operating systems and third-party software and hardware providers in order to avoid these firms 'self-preferencing' (i.e. prioritising their own products on operating systems / marketplaces they operate). In large part, the new interoperability requirements are focused at reducing anti-competitive practices rather than improving user experience, although that will likely be an indirect impact.

Standardisation and inclusiveness of technology is crucial for a successful metaverse. In order to achieve interoperability, it will be necessary to develop common global standards and protocols that underpin any statutory incentives for interoperability, through the investment in platform architecture and operations, wherein incentives are necessary to prompt organisations to make these outlays. This includes regulatory incentives and legal requirements for platforms to adopt a common approach that encourages frictionless economies, experiences and network effects as highlighted by WEF.[58]

Privacy by Design and Default

Privacy and personal data protection are crucial principles for the metaverse to ensure that users' rights are protected and respected as the metaverse expands and operates. Personal and sensitive data will play a major role in driving the expansion and operation of the metaverse, as platforms seek to leverage the identity of users to provide continuity of experience, tailored experiences, interoperability, and a sense of permanency and place. This includes personal information required to register accounts and create an online identity, as well as information about how a user is engaging with the service, any in-metaverse purchases, and possibly, their interaction with online marketing within the virtual environment and the merging of their data online. Additionally, if accessed via a VR medium, a host of unique biometric identifiers may also be processed to allow a user's avatar to navigate the virtual world.

Hence, the protection and management of personal data is of paramount importance, and it is essential that users are aware of how their data is being used and have control over it. Therefore, it is critical that privacy by design and default is integrated into all activities and business practices within the metaverse, from the design stage right through the entire data lifecycle, including hardware and software redundancy. The concept of privacy by design and default is one of the fundamental principles of privacy and finds mention in most data protection regulations globally. Broadly, 'privacy by design' requires that any handling of personal data must consider data protection and privacy at every stage, and 'privacy by default' requires that any product or service available to the public must apply the strictest privacy settings by default without need for any manual input from the individual. In this context, it is pertinent to note that leveraging privacy-enhancing technologies (PETs) (i.e. technologies that embody fundamental privacy principles by minimising personal data use, maximising data security, and empowering individuals) will be essential to comply with data protection principles and implementing privacy by design and default.

Having said that, it is however noted that any single

58 WEF (2023), Interoperability in the Metaverse https://www3.weforum.org/docs/WEF_Interoperability_in_the_Metaverse.pdf

experience may have multiple operators and users interacting in a shared space, each potentially collecting and using data, with requirements to notify users of intended processing and to establish a separate lawful basis for said processing, each of which are likely to be an extremely complex endeavor. It is therefore important to note that ensuring data protection in a metaverse environment is a shared responsibility, and all stakeholders should be aware of their responsibilities and obligations under data protection laws.

Sustainability by Design

Sustainability is an important principle for the metaverse to ensure that the environment and resources are protected as the metaverse expands and operates. This section focuses on the massive energy requirements for the metaverse to operate. As the metaverse relies heavily on computing power and technology, it is essential to consider the energy consumption associated with it. This is likely to be much higher than traditional digital applications which makes it even more important to urgently address this issue.

One way to address this issue is by implementing "energy saving by design" into the metaverse. This means that energy efficiency should be considered and integrated into the design of the metaverse, right from the start. Regulators may need to consider this principle and create guidelines for it.

Energy consumption can be reduced by using more energy efficient technologies such as renewable energy sources, or making better choices on more environmentally friendly options of cloud computing, edge computing and data servers. Governments should work with the private sector to determine not just the cost of computing and its environmental footprint (downstream and upstream) but encourage research and investment in more sustainable technologies through incentives, subsidies, and regulations. Another consideration for governments may be the need to ensure the balance between offsetting measures (such as carbon credits) and the diverse impact of metaverse enabling technologies on the environment.

Additionally, it is important to consider the lifecycle of the technology used in the metaverse and its effect on the environment. This includes the sourcing of materials, production, use, and disposal of the technology. It is important to ensure that the technology used in the metaverse is sustainable and does not harm the environment. Hence the metaverse should ensure sustainability by design.

Reciprocity

Reciprocity refers to the practice of mutual exchange between individuals or groups, wherein both parties benefit from the exchange. In the context of the metaverse, the concept of reciprocity may take a number of forms, including the exchange of digital assets and ideas between users, creators, developers and providers.

Adoption of the reciprocity principle within the metaverse community will promote trust and fairness by creating a culture where users and stakeholders are more likely to cooperate with each other, share resources and ideas, and work towards a common goal. This fosters a healthy and vibrant metaverse ecosystem that benefits everyone involved including practical benefits such as promoting innovation, collaboration, optimisation of resources and efficiency through knowledge sharing.

Achieving reciprocity in the metaverse requires a commitment from all stakeholders to act in a mutually beneficial manner. This can include the development of shared norms and values, as well as the creation of incentives and rewards that encourage reciprocity. For example, platforms may offer rewards to users who contribute to the community by sharing valuable insights, creating new content, or helping others. Similarly, metaverse operators may commit to reciprocity by establishing codes of conduct, standards and guidelines for behavior within the metaverse. This may potentially include enforcement of rules against harassment, cheating and other similar conduct. Metaverse developers may also promote reciprocity by sharing knowledge and expertise across multiple platforms. This may take various forms such as open-source code sharing, flagging incidents, vulnerabilities, and learnings, and collaborating on mutually beneficial projects. Reciprocity can also be supported by regulation and policy. For instance, regulations that promote data privacy and security can help build trust between users and platforms, while policies that incentivise open innovation and collaboration can encourage the exchange of ideas and resources.

Transparency for Trust

Transparency is a crucial principle for the metaverse to ensure that users are informed and aware of how the metaverse operates and the data it collects. This

principle encourages the development of products and services that are designed with user experience and expectations in mind, and that are transparent about their workings, user rights, and data collection practices.

One way to achieve transparency in the metaverse is by articulating best practices for responsible use and behavior when using products and services. Another way to achieve transparency is through policy prototyping. This involves assessing the impact of draft or early-stage policies and making improvements before wider adoption. This approach allows for a more collaborative, multi-stakeholder approach to addressing metaverse issues and ensures that policies are developed with the best interests of all stakeholders in mind.

Transparency also includes obliging online platforms to write their terms and conditions in a way that is accessible to the broader public and comprehendible to children. This will help users to understand what data is being collected and how it is being used, which will help them make more informed decisions about whether to use a particular platform or service.

Whistleblowing is another important aspect of transparency in the metaverse. It ensures that when violations of data protection, governance or other policies occur, there are mechanisms in place for individuals to safely and confidentially report or escalate these issues to the appropriate persons both internally at an organisational level or externally to an industry regulator and regulatory authorities.

Metaverse systems and technologies should also be designed and deployed to ensure their transparency. This may include transparency regarding any automated or artificial intelligence driven operations. This is to ensure that individuals can understand when they are impacted by an automated system and when an automated system is interacting with them.

Fairness, Equality and Inclusiveness

Fairness, equality and inclusiveness are critical to the ethical operation of the metaverse. Application of these principles ensures that all individuals have an equal opportunity to operate in the metaverse and there are no barriers for their entry into the metaverse. Metaverse systems and technologies should be able to demonstrate fairness towards individuals and that the outcomes do not infringe on their fundamental rights. Transparency and accountability can also be useful tools to promote fairness in the metaverse.

Metaverse systems should also not discriminate against any person or virtual representation of any person, and should allow for inclusive access to persons of all socio-economic backgrounds, abilities, race, ethinicity, gender, generational, religion, nationalities etc. This involves creating a virtual environment that is welcoming and accessible to all people without any barrier. For example, to ensure that the metaverse is accessible to users with disabilities, features such as text-to-speech or screen reader capabilities may be implemented.

Inclusivity in the metaverse can be promoted through inclusion of a diverse range of cultures, languages, and experiences within the virtual world and providing opportunities for users to connect and engage with one another in a manner that promotes respect, understanding and diversity.

Commitment to Diversity

Diversity, inclusion, and accessibility are crucial principles for the metaverse to ensure that the virtual world is inclusive and represents the diversity of the real world. These principles are necessary to promote gender, racial, generational, and ethnic participation in the metaverse, and ensure that all societies have access to metaverse technologies and are digitally literate.

Inclusive design is another important aspect of promoting diversity and inclusion in the metaverse. This means that metaverse technologies and services should be designed with the needs and perspectives of diverse populations in mind, and should be accessible to everyone, regardless of their abilities or background.

Given the digital divide, it is important to ensure that everyone has access to metaverse technologies and the opportunity to participate in the metaverse. This includes people in vulnerable and underrepresented communities, who may face barriers to accessing and participating in the metaverse. It is important to consider the needs and perspectives of these communities when designing and developing metaverse technologies and services.

To promote diversity and inclusion, policies need to be put in place that encourage and support participation from underrepresented groups. This can include initiatives such as digital literacy programs, mentorship and training opportunities, and funding for projects and startups that are focused on increasing diversity and inclusion in the metaverse.

As the metaverse becomes more ubiquitous, it is important to ensure that the virtual world is inclusive of the world's diverse populations. The metaverse has the potential to connect people from all over the world and bring them together in a shared virtual space. However, to ensure that the metaverse is truly inclusive and represents the diversity of the real world, it is important to consider the needs and perspectives of all communities, and put policies in place to promote diversity and inclusion.

Accountability

Accountability is an essential principle for the metaverse to ensure responsibility and accountability for metaverse systems, technologies and their outcomes including being accountable for any harm. Metaverse operators and other related stakeholders should be held accountable for any harm or unintended consequences. In other words, persons responsible for the different phases of the metaverse system lifecycle should be identifiable and accountable for the outcomes of the systems. The various mechanisms for accountability may include internal governance and control frameworks in place for monitoring systems, processes and projects regularly or external organisations auditing processes within the metaverse regularly, and enabling the assessment of algorithms, data and design processes. Additionally, operators must be held to account through laws, regulations, policies, and enforcement.

Another way to achieve accountability in the metaverse is by providing individuals with meaningful controls, where and when they matter. This means that research, not assumptions, is used to determine what controls are necessary, and they take into account context and sensitivity. This allows individuals to manage their experiences and how they use products and services within the metaverse. This also makes users and creators accountable for their choices in the metaverse.

Another way to achieve accountability is through the provision of key educational information to customers and decision makers. This information should be provided in a way that is easily accessible and understandable. It should explain how products and services work, what data is being collected and how it is being used, and what options are available to users for managing their experiences and data and how they can increase safeguards for themselves or their users.

Policies that offer recourse to users for violations, such as blocking or banning infringing users from the platform and confiscating their virtual assets, are also an important aspect of accountability. This ensures that users are protected from harmful or illegal activities within the metaverse.

Safety by Design and Beneficence

Safety by design and beneficence are essential principles for the metaverse to ensure that users are protected from harm, and that the virtual world is a safe and positive space for everyone. These principles involve a range of measures to protect users, including age and identity verification, parental or guardian control functionality, and mechanisms to investigate and prevent abusive activities.

One of the key measures to ensure safety by design and beneficence in the metaverse is age and identity verification. This is important to ensure that children, youth and the vulnerable are kept safe in the metaverse, and that platforms have the necessary mechanisms in place to verify the age[59] and identity of users. This also includes digital identity, which includes user agency and embodiment (avatar appearance) that must respect ethical principles and privacy.

Another important aspect of safety by design and beneficence in the metaverse is platform moderation. This includes measures to prevent online harm and prevent bullying, grooming, and addiction. Platform moderation will need to consider all elements of user behavior, including voice-driven, non-verbal, and behavioral content. At the same time, in line with fairness, there should be a duty of care to ensure well-being of the human content moderators. Where AI bots are being used to moderate human interactions, humans have a right to know.

User safety is also a crucial principle for the metaverse, and this includes hardware (such as VR headsets) as well as software components (platform and content moderation) to ensure users are not subject to sexual, racial or gender harassment. Online safety legislation is also important to ensure the safety of children and other vulnerable users in the metaverse. Coherent regulatory regimes are needed to minimise risks

59 Here the assumption is age is correlated to metaverse and digital maturity to navigate the experience.

while promoting, engaging and empowering play for children online as deemed appropriate by health, psychological, sociological and educational experts. This includes age verification, verified parent or guardian consent and controls, default settings, content moderation, anti-addiction, algorithmic accountability, and other specific requirements to protect children from harm. In addition, to ensure safety by design, excessive use controls should be implemented, such as obligatory "timeout sessions" or pop-up notifications that suggest taking a break.

The integrity and safety of user data, content, and assets is also essential, and this includes ensuring personal data protection and intellectual property guidelines are adhered to and that digital assets can be securely stored.

Additionally, mental well-being also needs to be considered as excessive use of metaverse can have negative effects on mental health on the individual and society, and hence there should be a focus on safety by design, excessive use controls and mental well-being to ensure a well-rounded safety and beneficence in the metaverse.

Conclusion

As the metaverse continues to grow at an exponential pace and progressively becomes a ubiquitous part of our day to day lives, the need for international consensus on standards for operation within the metaverse ecosystem increases. This paper summarises the tremendous opportunities the metaverse can bring and the areas we need to be better prepared for.

The metaverse is being embraced at various levels across diverse sectors such as manufacturing, healthcare, tourism, retail, creative economy, education, and financial services. However, in order for the metaverse to operate in a safe, transparent and ethical manner, there are several areas that need further dialogue as we have highlighted in our paper. These are further amplified by the lack of uniform regulation or code of conduct for operation within the metaverse.

Establishment of common minimum self-regulatory principles through international cooperation is one possible approach to counter this challenge. By working together to adopt self-regulatory measures that are effective, equitable and promote the safety and security of the metaverse users, the international community (namely, governments, industry and civil society) can help establish a global framework for responsible and sustainable growth of the metaverse. This can aid the global acceptance and legitimacy of the metaverse as a viable constituent of the global digital economy.

The self-regulatory principles that this paper has sought to enumerate may be a genesis that may be further built on by international cooperation. However, in order for self-regulation to be effective and enforceable, there is a need for proactive collaboration between governments, industry and other stakeholders.

Authors

UAE Minister of State for Artifical Intelligence, Digital Economy and Remote Work Applications Office
Saqr Binghalib
Marwan Al Serkal
Noora Al Malek

Mohammed Bin Rashed School of Government
Prof. Melodena Stephens

Dubai Future Foundation
Orkun Kirli

Dubai Economy and Tourism
Sahia Ahmad
Saif Al Rahma
Shanthi Thangaraj

Contributors

DLA Piper
Paul Allen
Kristi Swartz
Edward Chatterton
Amar Fahmy
Winson Lau

Pinsent Masons
Martin Hayward
Ruth Maria Bousonville
Tom Bicknell
Barka Doshi
Alexandra Bertz
Aliza Khan

Al Tamimi
Andrew Fawcett
Nileena Alexander

Access Partnership
Anja Engen
Hussein Abul-Enein
Melissa Govender

Cable Labs
Anju Ahuja

Accenture
Bahsar Kilani

World Economic Forum
Cathy Li

Dubai Virtual Assets Regulatory Authority
Deepa Raja Carbon

OKX
Dylan Voss
Nicole Purin
Akila Atapatthu
Tim Byun
Nicole Celine Lee

Remix Point
Genki Oda
Ryo Kato

University of Central Florida
Gregory Welch

PwC
Guy Parsonage

Yoti
Julie Dawson

Standard Chartered Bank
Lau, Su Kiang

Dubai International Financial Centre Authority
Lori Baker

Nokia
Marc Vancoppenolle

Microsoft
Nadim Hasbani

Luna PR
Nikita Sachdev

Binance
Steven McWhirter
Robbie Nakarmi

G42
Jonathan Lee

Observers

UK Department for Science, Innovation & Technology
Dr Katie Arthur

OECD
Miguel Amaral