BUSINESSatOECD THE USCIB FOUNDATION

PRIVACY, IMMERSIVE TECHNOLOGIES, AND THE METAVERSE

A JOINT REPORT OF *BUSINESS AT OECD* (BIAC)
AND THE USCIB FOUNDATION

ACKNOWLEDGEMENTS

The Privacy, Immersive Technologies, and the Metaverse special project is a joint initiative of *Business at OECD* (BIAC) and the United States Council for International Business (USCIB) Foundation, in support of ongoing analysis of the OECD Privacy Guidelines.

We would like to thank *Business at OECD* Members for their contributions to this report, and for their participation to roundtables held in Paris, Washington, D.C. and Kyoto.

We extend a special thanks to Paula Bruening, Founder and Principal, Casentino Strategies LLC, for serving as consultant to this project and the principle drafter of this Report, working together with Members of the ***Business at OECD*** Digital Policy Committee and invited experts from the field. We would also like to thank Steve Wood, former Chair of the OECD Working Party on Data Governance and Privacy, for his thought leadership and support of this project.

Business at OECD Established in 1962, *Business at OECD* is the officially recognized institutional business stakeholder at the OECD. We stand for policies that enable businesses of all sizes to contribute to economic growth, sustainable development, and societal prosperity. Through *Business at OECD*, national business and employers' federations representing over 10 million companies provide perspectives to cutting-edge OECD policy debates that shape market-based economies and impact global governance. Our expertise is enriched by the contributions of a wide range of international sector organizations.

The United States Council for International Business (USCIB) powers the success of US business across the globe. Our members include US-based companies and professional services firms from every sector of the economy, with operations in every region of the world. As the US affiliate of leading international business organizations including *Business at OECD*, The International Chamber of Commerce (ICC), and The International Organization of Employers (IOE), USCIB advances the US business perspective to policymakers and regulatory authorities worldwide and works to facilitate commerce, support sustainable development, and build trust in multilateral systems. USCIB is also the national guaranteeing and issuing association for ATA Carnets, a unified international customs document that allows for the temporary import and export of various types of goods into a foreign country without paying duties or taxes.

The USCIB Foundation is the research and education arm of The United States Council for International Business (USCIB). The principal purpose of the Foundation is to carry out activities designed to promote and advance the benefits of a free market economy and to demonstrate and document the role of the corporate private sector in economic growth and social development. The Foundation pursues that mission through a portfolio of initiatives that strives to inform future choices made by stakeholders and policy makers that benefit people around the world.

TABLE OF CONTENTS

EXECUTIVE **SUMMARY**

The metaverse promises an enhanced digital envi-ronment where individuals will work, play, connect, and collaborate. Built from the ground up by com-panies of all sizes, governments, and individual innovators, the metaverse will be an immersive, three-dimensional space that operates on multiple platforms and relies on shared data and technologies. In that space, people will interact with each other, with virtual objects, and with digitally rendered buildings, facilities, and landscapes. This new digital experience promises business opportunities across sectors and benefits across society. Organizations from a wide range of industry sectors - health care, education, manufacturing, public services and safety, and retail commerce - are investing in efforts toward implementation.

As companies explore the possibilities of the metaverse, they also seek to understand the novel privacy risks it may raise, and how those risks might be addressed. Realizing the promise of the metaverse will depend on fostering user trust through implementation and adherence to coherent, broadly accepted privacy governance frameworks that provide effective protections but do not impede innovation.

It is in this context that *Business at OECD* and the U.S. Council for International Business (USCIB) Foundation undertook this project to explore privacy issues raised by the metaverse, and to develop business-oriented evidence regarding the OECD Privacy Guidelines' applicability in this emerging environment, keeping in mind their two-part objective of protecting privacy and fostering cross-border data flows.

The Guidelines' broad cross-sectoral adoption, techn-ology neutral character and proven ability to support multi-stakeholder privacy solutions highlight their relevance to data governance for the metaverse. Moreover, the Guidelines' proven ability to provide a foundation for regulatory guidance - including the principle of Accountability's focus on implementation of privacy by design and privacy-enhancing technologies - position them to effectively address issues in the complex metaverse environment.

The collection and sharing of data will be central to implementation of the metaverse. While much of that data will not be personal and will raise no privacy issues, creation of user avatars that will populate the metaverse may require the collection of vast amounts of often sensitive personal data. In identifying the following, this study notes that in some cases privacy issues in the metaverse are novel, in others the metaverse may reinforce existing privacy concerns.

PRIVACY ISSUES

1. The volume and sensitivity of data collected in the metaverse may be unprecedented.

2. The processing of data in the metaverse could yield new, highly sensitive insights about individuals.

3. The new, powerful insights and profiles generated by the processing of sensitive data collected in the metaverse will reinforce existing questions about in what circumstances its secondary use is appropriate.

4. As it evolves, the metaverse will require significant data sharing to facilitate interoperability.

5. The metaverse may introduce practical challenges to compliance with existing data protection and privacy laws.

6. The metaverse will strain the ability to practically implement the OECD Privacy Guidelines' principles according to current norms of interpretation.

7. The global nature of the metaverse will present special challenges for compliance with children's privacy law.

8. Because the creation and function of the metaverse will rely extensively on AI, it may mirror – and possibly intensify - the privacy concerns AI raises, particularly with respect to fairness, bias and discrimination in automated decision-making or profiling.

9. The metaverse may prevent risks to privacy and resulting harms that cannot be currently foreseen.

RECOMMENDATIONS

In light of these issues, the report recommends that the OECD Digital Policy Committee, as a recognized convenor of multistakeholder dialogue and developer of consensus-based responses to policy challenges, consider advancing the following:

01

Deepen and broaden the evidence base regarding the relevance and applicability of the OECD Privacy Guidelines in the metaverse, including through practical case studies and multi-stakeholder dialogue-based research.

02

Map OECD instruments, reports, and ongoing work relevant to privacy in the metaverse, including initiatives related to AI, international data transfers, child safety online, data sharing and data portability.

03

Consider the role of regulatory sandboxes and their possible utility in understanding the strengths and limitations the OECD Privacy Guidelines as an oversight and policy development tool.

04

Ensure adequate consideration of the principle of Accountability and its role in effective data governance, and consider whether its workable deployment in the metaverse could benefit from additional recommendations that would complement existing guidance.

05

Explore how privacy enhancing technologies and privacy by design can be deployed to facilitate privacy in the metaverse. Identify ways in which the OECD Privacy Guidelines, particularly the principle of accountability, can support their implementation, effectiveness, and ability to mitigate risk and enhance individuals' privacy.

I. INTRODUCTION

The metaverse[1] will shape the future of the Internet[2]. As the next iteration in the online experience, the metaverse promises a digital environment where individuals will work, play, connect, and collaborate. The metaverse now is in its early stages. Today, users engage in immersive, three-dimensional experiences in discrete, independent digital spaces. In those spaces, people interact with each other, with virtual objects, and with digitally rendered buildings, facilities and landscapes. In the future, virtual spaces may be linked to create a metaverse potentially vast in its scale.

It is envisioned to be always on, so that experiences will be available to anyone who wishes to participate in them, and to include an unlimited number of users. By making virtual communication through gesture and voice possible, it may offer a more inclusive digital experience for people with special needs or those at varying levels of literacy. Users with disabilities or who interact with others in non-traditional ways may find support and community in the metaverse[3].

The origins of the metaverse are found in gaming, where as early as in 1986 multiple users participated in virtual, online environments and communities and interacted with characters in that world[4]. Today, the metaverse continues to be a work in progress. It is being built from the bottom up, through the creative efforts of companies of all sizes, governments, and individual innovators[5]. Its development relies on a combination of technologies, standards, platforms, and data.

While the future of the metaverse is yet to be fully understood and realized, and opinion about the course of its development varies[6], consumers and companies are experimenting and exploring its possibilities as a place for commerce and virtual learning, telemedicine and artistic expression, worker training and children's play. In 2022 companies invested $120 billion toward metaverse development – more than twice the resources they dedicated in 2021[7]. This investment in the metaverse and the immersive technologies that make it possible indicates business' understanding of the potential of this emerging digital environment[8].

The data necessary to build and operate the metaverse will be of greater quantity and more varied in kind than required in the current digital environment. Some of the data required will not be personal – data needed to create virtual landscapes or to emulate an interior space such as a house or a factory, for example, will not be linked to an individual. But in the metaverse, extended reality (XR) devices will gather personal data. That data will be processed to populate the metaverse with lifelike, interactive avatars and to personalize the user experience. Data will be gathered and processed continuously across time as individuals participate in the metaverse. This data will reveal, *inter alia*, what individuals do, with whom they associate, their preferences, and the way they participate in, and respond to, immersive experiences.

As companies explore the possibilities of the metaverse, they also seek to understand the novel risks it may raise, and how those risks might be addressed. Respect for users' privacy and the rights afforded them in data protection[9] will be critical to the user trust necessary to realizing the metaverse's full promise[10]. Workable data governance will be essential to establishing that trust. Such governance must be based on broadly accepted, coherent principles that provide effective, reliable protections and do not impede innovation.

Understanding and addressing the relevant privacy issues while the metaverse is still in its early stages may present the best opportunity to identify what existing measures provide real protections while encouraging innovation, and where additional work is needed to develop optimal solutions[11]. Past experience in law, governance and policy pertaining to the Internet and the online environment can serve as an important resource in understanding how to govern privacy in the metaverse.

Among the lessons learned is that privacy protections based in effective, agreed-upon, practicable principles can enable technology adoption and business growth. At the same time, it will be important to distinguish what existing and tested privacy solutions can work in the metaverse and where a one-to-one mapping of current approaches may prove not to be effective[12]. Recent proposals for AI governance that is flexible and scalable as the technology is developed and adopted offer helpful lessons at this early stage[13].

To that end, and in the context of the extensive work of the Organization for Economic Cooperation and Development (OECD) on the digital economy, the *Business at OECD* Digital Policy Committee together with the United States Council for International Business Foundation (USCIB) embarked upon this Privacy in the Metaverse and Immersive Technologies Project (The Project).

The Project was designed to contribute business evidence and insights in support of relevant workstreams undertaken by the OECD Digital Policy Committee in its ongoing program of work and to propose recommendations for possible future OECD analysis. Noting their long history as a recognized data governance instrument, *Business at OECD* and USCIB centered the Project on the OECD Privacy Guidelines (the Guidelines)[14] as the critical privacy reference for the work. The Guidelines' broad acceptance and adoption, their translation into law and regulation, and their ability to support risk-based governance and accountability have enabled their workability over a period of rapid technological change. This demonstrated durability and adaptability position them to serve efforts to understand and address the need for data governance in the emerging metaverse. Moreover, the convening function of the OECD has long facilitated development of multistakeholder, broadly agreed-upon data governance solutions of the kind needed in a digital environment created and used by a vast number of diverse entities and participants. The OECD's ongoing work on issues and technologies relevant to privacy in the metaverse[15], particularly in the areas of AI governance, privacy enhancing technologies, and protection of children in digital spaces, illustrates its unique role in this regard.

II. PROJECT GOALS **AND PROCESS**

Recognizing business's interest in the tremendous potential of the metaverse and related immersive technologies, and the critical role data and data flows will serve in creating it, *Business at OECD* and the USCIB Foundation launched this Project to examine specifically the issue of privacy in the metaverse. The Project was designed to consider the extent to which the metaverse may pose unique privacy and data protection issues, and how they might be addressed in the context of the Guidelines. It focused on both the benefits the metaverse promises and the risks to privacy it may raise, keeping in mind the Guidelines' two-part objective of protecting privacy and fostering data flows. The goal of the Project was to develop and deliver to the OECD business-oriented evidence that would suggest whether additional work was necessary to address the applicability of the Guidelines in the metaverse, and questions the OECD might consider in its deliberations.

The Project included an inaugural meeting and a series of three Roundtables, each of which brought together experts to consider questions about the promise of the metaverse, business's motivation for investment, and key privacy issues. Participating experts represented industry, academia, and public policy. Representatives of civil society also were called upon to raise and respond to questions about privacy and governance in the metaverse, and to highlight the need to address these issues in the context of other relevant concerns such as ethics, human rights, mental health, environmental sustainability, and child safety[16]. Participants also stressed the importance of providing content users and developers the opportunity to gain metaverse skills and literacy[17]. The OECD presented some of the relevant OECD work activities to provide context for the Project.

THE ROUNDTABLES

The Project centered upon a series of four Roundtable discussions designed to explore the business perspective on the metaverse's potential, the privacy issues the metaverse may raise, and the applicability of the OECD Guidelines as a governance tool.

The Roundtables surfaced privacy and related issues; highlighted the business motivation for investment; and reviewed the benefits the metaverse may offer across society. Discussion also focused on whether the workability and relevance of the Guidelines would benefit from future work by the OECD.

The Roundtables were convened under Chatham House Rules both in person and online to encourage candid discussion by the broadest possible range of stakeholders.

LEAD-OFF ROUNDTABLE

Gran Canaria, December 15, 2022

The Lead-off Roundtable brought together business and other stakeholder experts for a moderated discussion about privacy issues raised in the metaverse. At the meeting, *Business at OECD* and the USCIB Foundation outlined plans and goals for the Project. Through moderated exchange the Roundtable elicited business' vision for the metaverse, what challenges companies may face when complying with privacy laws and regulations, and how those challenges might potentially impede the ability to realize the metaverse's greatest potential.

ROUNDTABLE I

Paris, May 9, 2023

Roundtable I convened business and other stakeholder experts to begin consideration of data privacy issues raised by the metaverse and immersive technologies. The meeting provided an opportunity to consider a vocabulary and structure for talking about the metaverse in the context of data privacy; concrete examples of business investment; and use cases that illustrated the data infrastructure and data flows essential to the creation and function of the metaverse.

ROUNDTABLE II

Washington D.C, June 27, 2023

In Roundtable II, participants focused on data governance issues raised by the metaverse and the application of the OECD Guidelines to address them. Using concrete examples of business implementations, experts highlighted how the OECD Guidelines remain relevant and useful; the extent to which they are likely to continue to serve their intended purpose in the metaverse; how they may be effectively applied to this particular context; and where their application is challenged by the realities of technology, data, and data processing in the metaverse. Participants also discussed whether the Guidelines might require review or reinterpretation to ensure their continued relevance and practical utility.

ROUNDTABLE III

Kyoto, October 9, 2023

Roundtable III was organized to coincide with the meeting of the Internet Governance Forum to benefit from the contributions of the broad range of stakeholders present for that meeting. It was also intended to highlight the perspective of representatives of Japanese business and government. The Roundtable discussion centered on presentations and questions related to Japan's perspective on data governance issues and possible solutions for privacy in immersive technologies and the metaverse. Remarks drew upon examples from Japan other Asian countries of policy-related initiatives and considered the relevance of the APEC Privacy Framework to data governance in the metaverse.

Presentations included use cases illustrating the promise of immersive technologies; predictions of societal, governmental, and commercial benefits; and forecasts about anticipated economic growth and business investment in the Asia-Pacific region. Speakers identified how data governance can address privacy privacy issues while enabling and supporting innovation, implementation, and adoption.

The Roundtable discussions were wide-ranging. At early meetings, participants focused on understanding the scope of the metaverse and the technology, standards, and protocols that would make its creation and operation possible. They also examined the promise and potential of the metaverse and the motivation for business investment. Discussions turned to specific privacy and data protection issues raised by the metaverse and the relevance of the OCED Guidelines to governance. The final Roundtable, convened in Kyoto, placed special emphasis on Asia-based companies' metaverse-related innovation related and the relevance of the APEC Privacy Framework.[18]

In addition to the Roundtables, the Project secretariat engaged in research to supplement and further explicate the information and issues surfaced during Roundtable discussions. To explore in greater detail questions related to the policy challenges related to application of the Guidelines in the metaverse, *Business at OECD* conducted a series of guided discussions with experts. Finally, the *Business at OECD* secretariat met one-on-one with stakeholders to solicit advice and to engage in discussion focused on key issues.

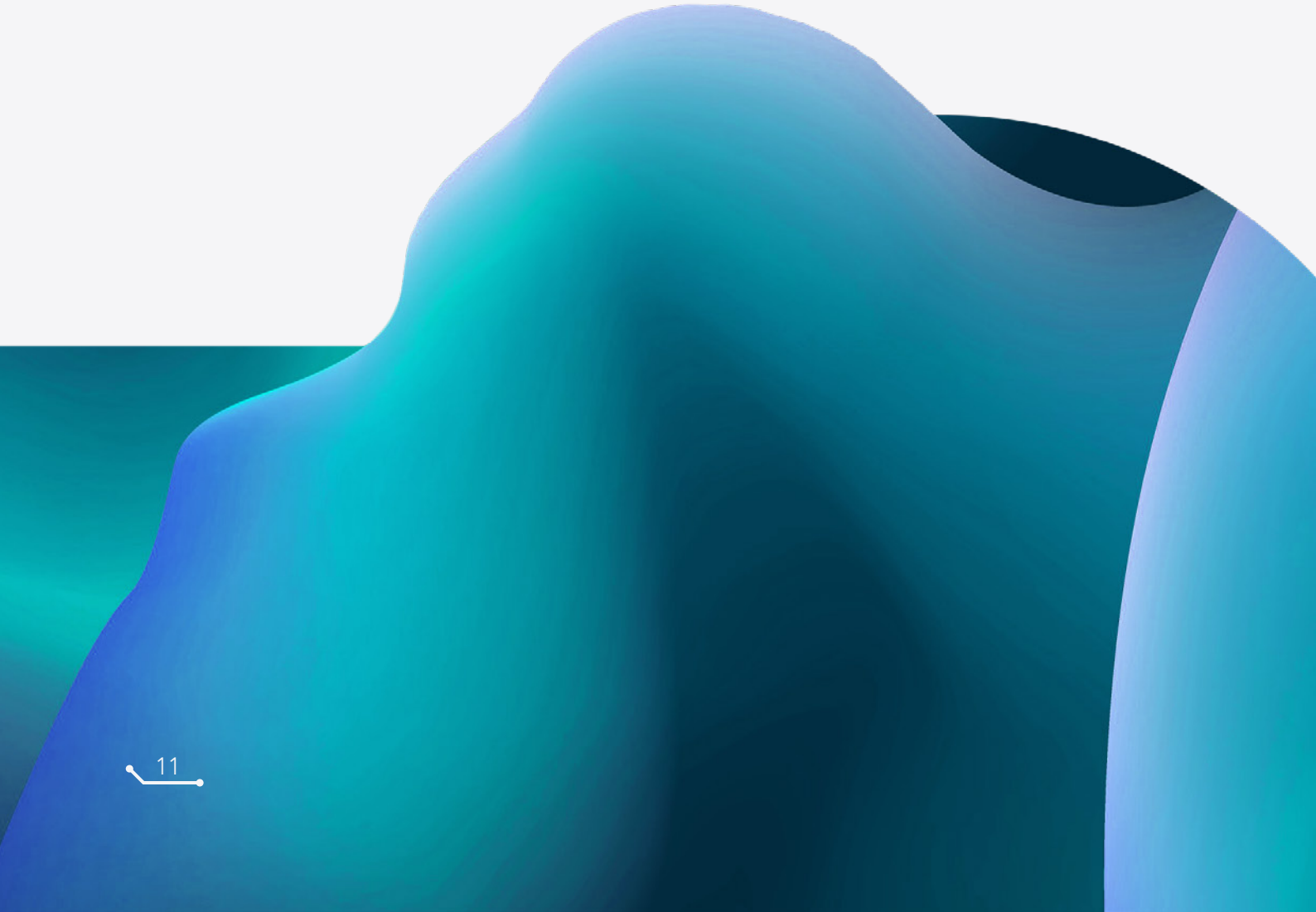
The meetings were convened in-person and online to encourage the broadest possible participation and cross-sectoral representation. All discussions were governed by Chatham House Rules to encourage candor and open discussion. Each Roundtable was followed by a public reporting document that highlighted key themes, presentations, and interventions.

III. WHAT IS THE **METAVERSE?**

Visions of what the metaverse is - and what it will become - vary. Some experts anticipate a massively scaled[19] network of digital spaces that will enable immersive, three-dimensional experiences. Others envision virtual environments and experiences that, while also immersive and three-dimensional, are discrete and independent. The metaverse will develop as technology advances and user demand grows, and as new possibilities for what it can offer emerge. It is important, therefore, when considering what the metaverse is, to bear in mind its innovative, evolving character.

Metaverse spaces, supported by augmented, virtual, and mixed reality, will bridge the online, offline, and physical worlds[20]. While today these discrete digital spaces may exist in isolation, they are envisioned one day to be in some cases interconnected and interoperable[21], enabling users to move between them seamlessly. The result will be a digital world in which people can avail themselves of a range of immersive experiences[22].

The experience of the metaverse is often distinguished from that of the existing Internet by its sense of "presence." While currently users experience the digital world through screens, the metaverse will provide an immersive experience where they will interact with other users, virtual objects, and the digital environment. Any number of people may participate in an immersive experience, all at the same time. Supported by secure, sustainable networks, metaverse environments will be potentially always on and persistent; users will be able to leave and return to experiences and to access them as long as they are made available. The environment will enable people to connect, communicate, and engage with others and digital content in ways that once were not possible. In doing so, it is anticipated to open new avenues for entertainment, business, commerce, communications, and creative collaboration in virtual spaces[23].



DATA COLLECTED IN THE METAVERSE

Body-based data includes data about unique physiological characteristics or movements, such as eye tracking or other body motion. This data is necessary to calibrate headsets and prevent motion sickness during an immersive experience. Users interact with virtual content based on data about eye movement and where they direct their gaze.[24]

Biometric data are measurable physical, physiological, or behavioral characteristics used to recognize or verify an individual's identity. Facial images, fingerprints, and iris scan samples are all examples of biometrics.[25] Other physical biometric data may include retinal analysis, voice recognition, iris scanning and ear shape recognition. Behavioral biometric identification techniques include analysis of keystroke, handwritten signature, gait, and gaze.

Inferred data is widely agreed to be data that is the output of processing, rather than data that is provided directly or indirectly from a person.[26] Inferred data often may be predictive or be part of a profile. Inferred data is distinct from data that is gathered purely through direct observation that has not been processed or combined with different data sets.[27]

Geospatial data includes information related to locations on the Earth's surface. Similarly, geographic data and information is defined in the ISO/TC 211 series of standards as data and information having an implicit or explicit association with a location relative to Earth. Geospatial data may be relatively static – e.g., a natural or man-made disaster site, the location of a building project; it may also change, in the case, e.g., of movements of vehicles or the spread of diseases. Geospatial data typically incorporates spatial data gathered from many diverse sources in various formats. It can include, for example, census data, satellite imagery, weather data, cell phone data, drawn images and social media data.[27]

Psychographic data refers to information about attitudes, aspirations, values, personality traits, and other psychological criteria. Psychographic data can be used to build a profile of how an individual views the world, the things that interest them, and what motivates them. It relates to a person's activities and opinions. Psychographic data is distinguished from demographic data which may include population, race, income, education, and employment.[30]

Digital asset data – A digital asset is generally anything that is created and stored digitally, is identifiable and discoverable, and has or provides value. Data, images, video, and written content, are examples of digital assets.

One aspect of the metaverse will be its reliance on interoperability within and between immersive environments, including interoperability of relevant technologies and networks. When necessary, interoperability will enable users to transfer settings, preferences, data, and the value they create from one platform to another without barriers. It also will allow users to move their data assets from one platform to another and to share or sell it to other users. It is important to note, however, that there also will be instances when immersive technologies and environments will not be linked.

THE ELEMENTS OF THE METAVERSE

Several key elements will support the metaverse experience. Among these will be avatars; digital twins; artificial intelligence; data and data sharing; sensor technology; and standards and protocols.

AVATARS AND DIGITAL TWINS

In the metaverse, *avatars* and *digital twins* will enable users to interact with each other and with digital objects, landscapes, and environments in industrial, individual, and commercial contexts. *Avatars* are on-screen, 3-dimensional, virtual representations of users in virtual worlds.[31] Their actions and decisions mirror those of the individual they represent. An avatar will serve as an identification document by which a user establishes who they are. Avatars likely will be custom-tailored to the individual, highly realistic, and able to closely resemble users' facial and physical features.[32] Avatars will reflect a user's psychology, emotions, and mental state.

Digital twins may be thought of as virtual representations of physical objects or devices (such as a table or a lamp), or a process (such as in manufacturing). The twin comprises data collected from multiple sources[33], behavioral insights inferred from the data, and visualizations. The digital twin can serve as the foundation for development of use cases, simulations, and additional visualizations. A digital twin might, for example, replicate the operations of an assembly line or the flow of traffic through an area of a city. Based on these, the digital twin could yield insights about how these might be improved or enhanced. What the metaverse reveals about, for example, how well a company's equipment is working, how resources and staff are deployed, or where inefficiencies in the flow of production or vehicles might be occurring, will inform decisions about when and where changes might be needed.[34]

DATA AND DATA SHARING

Data is essential to the infrastructure of the metaverse and to creating immersive virtual experiences. Data collection and processing will be necessary to render and deploy digital twins. Historical and current data from various sources will be needed to architect and maintain up-to-date representations of a physical space, entity, or environment.[35] Data will in many cases fuel the AI required to build avatars, to personalize user experiences, and to optimize virtual worlds.

Creating a digital twin that emulates the physical infrastructure of a factory or health care clinic would not require personal data. But to create an interactive avatar, operators will in some cases need to collect highly sensitive personal data related to users' bodies – their eye movement, vocal inflection, heart rate, and blood pressure. Creating a successfully convincing avatar will in some cases require monitoring of users' gait, head and body motions, and posture. Organizations will process data using machine learning algorithms and artificial intelligence techniques to derive inferences about them. This collection and processing intensify the data collection model already applied on the Internet, which in many cases (e.g, personalized services, including social media) relevant data is collected about the user and their activity from their devices in addition to the data the user may themselves provide.

Sharing of personal data may also in some instances be essential to fostering interoperability. Building and operating the metaverse will involve a variety of platforms, technologies, companies, organizations, and users. To support some of the desired metaverse experiences, these will need to be interoperable, so that users can move easily between these different environments. Their avatar must be able to travel, move assets, and when necessary, maintain their digital identity from one virtual space to another. To make this possible, the data required to create the avatar will be shared or linked between these different spaces and the entities that make them run.[36]

ARTIFICIAL INTELLIGENCE (AI)

AI's role in powering the metaverse is predicted to expand as the environment grows and develops.[37] According to the International Telecommunications Union (ITC), AI may be the most essential element of the metaverse because of its ability to generate the new text, images, video, audio, 3D models and computer code necessary to building virtual worlds and personalizing experiences.[38] While the extent of AI's role in creating the metaverse is not fully understood, it likely will play a significant role in determining how the metaverse develops and the nature of the experiences available there. It will be particularly critical to generating new virtual content, building dynamic virtual worlds, and personalizing experiences.[39]

AI will be central to the creation of the avatars that populate the metaverse. It will make it possible to custom design their appearance, traits, and behaviors, making them a more convincing reflection of the users they represent.[40] Supported by AI, avatars will interact with each other and with digital twins. They will be able to answer questions, provide insights, and in some cases engage in natural language conversation, so that interactions in the metaverse will be believable and engaging. Advanced AI will enable avatars to detect user emotions based on their interactions, vocal inflection, or facial expressions so that they can respond intelligently and empathetically, adjusting their behavior and dialogue to suit various environments and the user's emotional state.

AI also will be critical to the development of digital twins. It will assist in the creation of landscapes (such as spaces in nature) and *environments* (such as houses, offices, and factories). It will also be essential to creation of three-dimensional *digital assets* such as chairs, desks, or machines. AI will make it possible for users to change virtual spaces in response to decisions and to suit their interactions and activities. A couple may, for example, experiment with alterations and enhancements to their home in the metaverse to accommodate the arrival of children or limitations on their mobility as they age. Management may redesign a factory environment in response to production needs or safety measures. Library staff may change meeting spaces as patrons' needs evolve.

Finally, AI will enhance and custom design the individual user's experience of the metaverse. By analysing user data - from basic profile information to intricate behavioral patterns, user needs, and preferences - AI will tailor virtual environments to the user's preferences.[42]

SENSORS

Sensory interfaces, applications and infrastructures will be essential to the metaverse. Sensors will connect the digital and physical worlds by processing data so that it can be translated into digital representations and interactions.[43]

Sensors include a diverse array of technologies, including cameras, accelerometers, gyroscopes, depth sensors.[44] As a tool that enables the monitoring, tracking, and replication of users' movements and actions in the digital environment, sensors enhance the ability of users to feel present and immersed in the metaverse. Sensor-enabled hand tracking, for example, makes it possible for users to manipulate digital objects using natural hand gestures. By tracking where the user is looking, sensors can enhance the quality of the user interface and enable more realistic interactions.[45]

STANDARDS AND PROTOCOLS

To create and sustain an interoperable metaverse, developers will adhere to common standards, protocols, and frameworks that facilitate data sharing across domains and platforms.[46] The metaverse also will require agreed-upon functionality and rules to enable interoperable assets that can be used across virtual worlds.

IV. BUSINESS INVESTMENT AND PROJECTIONS FOR **ECONOMIC VALUE IN THE METAVERSE**

The rate of investment in the metaverse and the immersive technologies required to build it highlights the potential companies have identified in creating and doing business in this environment. Investment may take many forms, including training for developers and users to enhance their ability to create and participate in the metaverse; development of high- quality content; and research, particularly into questions of governance, health, and safety.[47] This investment can be seen across three categories of investors: large technology companies, venture capital, and corporations and brands outside of the technology sector.[48] Companies across all sectors are investing in industrial, enterprise, and consumer-facing applications.[49]

According to a McKinsey report, more than $120 billion were directed toward development of the metaverse in 2022 – more than double the $57 million invested in 2021. McKinsey suggests that the metaverse may generate up to $5 trillion in economic impact by 2030 – equivalent to the size of the world's third largest economy, Japan.

Because of its potential to enable new business models, products, and services, and to act as a means for businesses to reach consumers, the metaverse may become the biggest new growth opportunity for several industries over the coming decade.[50]

The Analysis Group in 2022 released a report predicting that if metaverse adoption and impact evolve similarly to mobile technology, it could contribute 2.8% to global gross domestic product (GDP) in the 10th year after adoption begins. The report forecasts that the metaverse could have applications that extend across the marketplace, with the potential to transform diverse sectors of the economy: education, health care, manufacturing, job training, communications, entertainment, and retail.[51]

V. OPPORTUNITIES IN THE INDUSTRIAL, **ENTERPRISE AND COMMERCIAL METAVERSE**

The metaverse and relevant immersive technologies promise opportunities across industry sectors. In addition to the discussion below, use cases that describe specific applications may be found in the Appendix to this document.

THE INDUSTRIAL METAVERSE

The *industrial metaverse* is a digital recreation of the infrastructure of the physical world, and a simulation of the places, vehicles, equipment and machines used there.[52] It holds the potential to revolutionize city planning, delivery of services, workplace safety, emergency response and disaster relief.[53] By making it possible for governments, businesses, and NGOs to model and test their tools, systems and processes, the industrial metaverse may provide new avenues for problem solving and enhance delivery of effective solutions.[54]

For example in the metaverse, first responders will prepare for real-world incidents that can be anticipated but cannot be trained for.[55] Firefighters will be able to see and visualize in real time what is occurring in dangerous situations, and to make better, often life-saving decisions about their course of action.[56] The metaverse will also provide opportunities to supplement traditional police training, equipping officers with skills to handle complex, challenging, or unpredictable situations.[57]

The metaverse will provide developers of urban spaces and public buildings with opportunities to address issues of accessibility early in the design process. Virtual tools will equip them to understand the needs of people with disabilities and to identify ways to accommodate them in houses, apartments, office buildings, parks, transportation systems and other public and private spaces.[58]

The metaverse will offer platforms that support prediction, management, and response to natural disasters, equipping agencies to assess risks to various regions, facilitate evacuation and coordinate disaster response.[59]

THE ENTERPRISE METAVERSE

The *enterprise metaverse* connects digital twins of every aspect of an organization to enable virtual collaboration, training, and skills development.

Collaboration in the enterprise metaverse will help companies evaluate the need for equipment maintenance, repair, or replacement, minimizing production interruptions and supply chain disruptions.[60] In the enterprise metaverse colleagues and experts will be able to virtually assess emergency situations and dangerous manufacturing environments to determine how to address them. Data generated by metaverse simulations will support business planning and decisions about, for example, changes in production capacity, consumer preferences, and market demand.[61]

The collaboration enabled in the enterprise metaverse also promises a new platform for health care delivery and training medical professionals. It will expand upon the current delivery of telemedicine and enhance the ability of providers to provide services at a geographic distance. It also will support the use of digital models of patients that can be used to test the efficacy and forecast the impact of various courses of treatment.[62]

The metaverse provides a platform and tools to help physicians prepare and plan for surgery by enabling them in advance to see and consider complex medical conditions in a 3-dimensional, immersive way.[63] It enables doctors to visualise the anatomy of their patients and procedures in real time, allowing for greater precision in surgical procedures. In some cases, it will enable doctors to advise in surgeries conducted in other geographic locations, making available to patients in remote areas the most current procedures.[64]

The metaverse offers opportunities for practical education for medical professionals, allowing students to research, train and practice on virtual models. In virtual classrooms, students equipped with virtual reality (VR) software visualise and understand the intricacies of the human body.[65] Because the metaverse does not require the physical space, equipment, and human remains traditionally used to study anatomy, it affords a broader range of students preparing for health care professions – at both the undergraduate and graduate level – the opportunity for intensive study and understanding of the human body.[66] This capability also will be available for students as part of their pre-university science education.[67]

The metaverse will also make education resources available to students otherwise unable to access traditional classrooms and bring together students from diverse geographical locations.[68] Virtual classrooms will allow students and teachers to interact with one another in a virtual space; participate in customized activities in breakout rooms; play educational games; visit libraries, museums, and historical sites; hear visiting speakers and lecturers; and attend classes. The metaverse is expected to offer an array of alternative approaches to education predicted to motivate students across a variety of learning styles and increase student engagement. It will enable collaborative teaching that augments the traditional learning experience.[69]

In the metaverse teachers will tailor pedagogy to the individual student and adapt it to their learning style. With the help of immersive media and technologies, the metaverse may accommodate students with special educational needs and disabilities by lowering or eliminating barriers to their access to resources[70] and improving their online learning experience.[71] Metaverse platforms' ability to make available bespoke virtual learning materials and environments can also benefit learners with autism and other special needs, such as reading and hearing disabilities.

THE COMMERCIAL METAVERSE

The metaverse presents opportunities for virtual commerce and retail. As in the physical world, businesses will offer products and services in the metaverse – building real estate, manufacturing cars and clothing and office equipment, and creating experiences. Users will determine the market for what they purchase, own and experience in the metaverse.[75] Businesses will also use metaverse e-commerce to create personalized, immersive experiences for its customers.

In the commercial metaverse, businesses also will enhance and expand the online shopping experience. Virtual storefronts and showrooms will enable companies to showcase their products in ways not possible on a two-dimensional screen and to enrich and enhance their current offerings.[76] Customers will experience remotely in-person shopping replicated in metaverse storefronts[77], empowered by virtual tours, fittings, and the services of virtual assistants and AI chatbots to make more informed choices.[78]

VI. PRIVACY ISSUES IN **THE METAVERSE**

While the transformative promise of the metaverse is evident, implementation of the technologies and data processing methods required to create it raise privacy issues. Addressing these concerns will be critical to establishing the trust necessary for its adoption and individuals' willingness to engage in activities there.

01 THE VOLUME AND SENSITIVITY OF DATA COLLECTED IN THE METAVERSE MAY BE UNPRECEDENTED.

The amount of data required to create and operate the metaverse is expected to be vast.[79] Organizations that create and operate in the metaverse will collect more kinds of data, and in greater volume. This expanded collection could be sustained over long periods of time as users engage in the metaverse as a regular activity, in personal or professional contexts.

In many instances, the data needed will be neither personal nor sensitive. The data required to build digital twins of machinery or to replicate the architecture of an environment, for example, is not related to individuals and poses no threat to individual privacy. But in other cases, the data collected will be directly or indirectly linked to users. Some personal data may differ little from that currently collected – *e.g.* data for registration and authentication to access a resource, service, or activity, to facilitate delivery of services, or to enable an account log-in. But enabling users to function in the metaverse also will require the collection and processing of large quantities of a broad range of highly sensitive personal data about them, most notably body-based and biometric data. This may include, for example, real-time data about an individual's vital signs, gait, facial image, voice, gaze, and posture. It may also involve data about sensations and interactions in the metaverse with other individuals, physical surroundings, content, and objects.[81]

02 THE PROCESSING OF DATA IN THE METAVERSE COULD YIELD NEW, HIGHLY SENSITIVE INSIGHTS ABOUT INDIVIDUALS.

Processing of sensitive body-based data may be necessary to the function of certain immersive experiences. Data tracking a user's gaze may be processed to accurately render what they should see; biometric data such as facial features or retinal scans may in some instances be used for identification. Vital signs may be analyzed to reveal a user's reaction to a situation or interaction. Inferences drawn from this data can reveal deeper insights about an individual's mental or emotional state, their physical health, their likelihood to engage in certain kinds of activities, and their tastes and interests. Analysis of data collected in the metaverse also may compromise attempts at user anonymity[82] and could yield insights into the collective reaction of communities of users.[83]

03 THE NEW POWERFUL INSIGHTS AND PROFILES GENERATED BY THE PROCESSING OF SENSITIVE DATA COLLECTED IN THE METAVERSE WILL REINFORCE QUESTIONS ABOUT IN WHAT CIRCUMSTANCES ITS SECONDARY USE IS APPROPRIATE.

The highly sensitive data collected in the metaverse and the powerful new insights it makes possible will be of interest to organizations across all sectors of society. Profiles derived from body-based and biometric data could inform health science research and insurance decision-making. Insights about children's attention span and response to education materials could be used to design classrooms, lesson plans and custom-tailored learning for individual students. Psychographic data could provide companies with a deeper, more precise understanding of preferences and buying habits, raising questions about targeting advertising to individual users based on the powerful, highly sensitive insights and inferences this data yields. Organizations of all kinds will be faced with choices about the secondary use of this data and establishing criteria for determining when such uses are appropriate.

04 AS IT EVOLVES, THE METAVERSE WILL REQUIRE SIGNIFICANT DATA SHARING TO FACILITATE INTEROPERABILITY.

As discussed above, the metaverse will be built across interoperable platforms and networks, and will require the collaboration of companies, governments, innovators, and individuals. Facilitating interoperability in the metaverse will require extensive transfers of data. Creating the level of personalization needed to provide the intended user experience and enabling users to move between different spaces in the metaverse also will require sharing of data between those spaces. Because the metaverse will enable movement between immersive environments, users will potentially bring avatars, wallets, contacts, and in some cases the history of their activity with them as they travel across virtual spaces. As they do, platforms will need to identify and authenticate them for authorized access to experiences and activities such as health care or education. Data sharing will also be necessary to facilitate trusted transactions in the metaverse. Given the highly sensitive nature of data collected in the metaverse, decisions about what data should be required for identity verification and authentication in what circumstances could have significant implications for privacy.

Managing this data sharing and ensuring that individuals are afforded protections and the necessary level of control as data moves across the metaverse raise significant governance challenges. Moreover, these transfers may occur across jurisdictions, where legal requirements with respect to data protection may vary. Approaches to governance will need to reflect the metaverse's anticipated global reach and the desire of users to move within it. It will also be important to avoid introducing friction that may reduce user interest if the metaverse's usability is significantly impaired. Ideally, practical governance will encourage both innovation and protections for users.

05 THE METAVERSE MAY INTRODUCE PRACTICAL CHALLENGES TO COMPLIANCE WITH EXISTING DATA PROTECTION AND PRIVACY LAWS.

While the metaverse in its current early stage consists of distinct, discrete virtual environments, some visions of its future involve an extensive, complex network of entities and relationships across which data will be collected, shared, and processed. This complexity will challenge existing approaches to data protection law, which designate responsibility for aspects of data governance based on whether an entity functions as a "controller" or a "processor."[84]

The future metaverse also may challenge the ability to identify what entity is responsible for honoring individuals' rights in their data. The right to access, correct, amend, or delete certain data is articulated in the Guidelines and codified in many countries' data protection laws. Given the complexity of the metaverse, it may be difficult to determine which individuals are provided such rights under law. The metaverse also may challenge companies' efforts to notify individuals about what entity is responsible for responding to their requests to exercise those rights, and how that entity can be contacted.[85]

The metaverse also could further complicate the question of what data protection laws apply. The robust flows of data required to operate the metaverse will be shared across jurisdictions whose data protection regimes may vary in their requirements. Understanding what country's data protection laws govern a particular instance of data collection, processing or sharing may challenge organizations' ability to reconcile compliance across jurisdictions.[86]

06 THE METAVERSE MAY STRAIN THE ABILITY TO PRACTICALLY IMPLEMENT THE GUIDELINES' PRINCIPLES ACCORDING TO CURRENT NORMS OF INTERPRETATION.

Because of the rich complexity of the metaverse environment – e.g., the volume and sensitivity of the data required to implement it, the network of interoperable platforms and technologies necessary to support it, and its reliance on AI, individuals and organizations involved in its creation and implementation of will face significant challenges as they attempt to comply with the fair information practice principles reflected in the Guidelines.[87]

The Guideline's principle of Openness, which is commonly referred to in terms of transparency, provides an illustrative example. Openness will be fundamental to establishing immersive environments and experiences that respect users' privacy. Organizations in the metaverse will be tasked – as they are today in the physical and digital world - with informing users about what information will be collected and how it will be used at the time they enter an environment, engage in an activity, or make a purchase. Ideally, this notification will occur within the broader context of user education: the public will be provided with resources to help them understand data practices in the metaverse more generally; when and how they can exercise control over their data; and how they can exercise their rights in data (e.g., to access, correction, and amendment) as established in law and regulation.

Given the breadth, variety and sensitivity of the personal information collected, inferred, and processed in the metaverse, providing notices that are useful to individuals may be difficult at best.[88] As data collection, sharing and processing has become more ubiquitous and complex, practitioners have struggled to create privacy notices that meet existing regulatory requirements that they be clear, comprehensive, and understandable to the public. While the demands of the metaverse will likely compound those challenges, it also may offer new ways to address them.

Moreover, implementation, growth, and refinement of the metaverse will rely heavily on AI, a processing method that presents its own significant challenges to transparency. Most organizations adhere to the Purpose Specification principle by providing an explanation of the purpose of collection, usually in a privacy notice. AI's ability to derive meaning from data beyond what it was initially collected for significantly challenges this principle. In some cases, organizations may not necessarily know at the time of collection how the information may be used by AI in the future. Because the Use Limitation principle endeavors to ensure that personal information is only used for the purpose for which it was collected, organizations may wish to avoid limiting its opportunities to use data in various ways it may not have initially anticipated. They instead may be motivated to broaden any articulation of purpose in privacy notices to allow for collection of data even when its utility, particularly in AI, is not immediately clear.

It also is not clear to what extent notification and education can provide users with sufficient information on which to base informed consent to the collection and use of data in the metaverse. Significantly, consent to data collection may not be required in every instance – the Guidelines' principle of Collection Limitation specifies that consent should be obtained "where appropriate." Where it is not required, other mechanisms, e.g., a company's legitimate interest, may be available to mitigate the risk of harm and establish the basis for responsible data use. In such cases, while some transparency is still necessary to promote Openness, the degree of disclosure needed may not reach the level required when it is intended to support informed consent. However, when informed consent is sought in the metaverse, providing the transparency necessary to support it may be difficult. While it may be possible to articulate the kinds of data that are collected, and the uses to which it will be put, much of the data – biometric, geospatial, body-based – will be highly sensitive, and may be processed to yield even more sensitive inferences. The nature of this data and processing may test organizations' efforts to convey to the lay reader the significance of this kind of data and the implications of its collection.

The goal of the metaverse experience – that it be immersive and that users move across platforms and spaces seamlessly - could be compromised by the need to consent repeatedly to data collection and use. It may also be the case, however, that the unique nature of the metaverse and immersive technologies may present opportunities for enhanced user education and tools for effective notification, such as user experience capabilities that have not been available in the current digital experience. The AI that supports the metaverse may offer solutions to the issue of user consent, by "learning" a user's data collection and use preferences and putting that preference into effect across an experience or connected experiences.

Moreover, it is important to bear in mind that AI – a method of data processing on which the metaverse will depend - relies on ingesting great quanitities of data to train and test algorithms. Collecting data in such large quantities can assist the development of AI, but it can also conflict with the Collection Limitation principle Limits on the collection of personal information may practically conflict with efforts to develop and enhance the functionality of AI and in doing so, limit the potential of the metaverse - the quality of the experiences there and the potential it may hold for industry, government, and society at large. In the metaverse, it may be necessary to interpret the principle of collection limitation in the context of the data's use to distinguish when large scale collection may be necessary to accomplish some legitimate purpose from when such collection is indiscriminate.

07 THE GLOBAL NATURE OF THE METAVERSE WILL EXACERBATE EXISTING CHALLENGES FOR COMPLIANCE WITH CHILDREN'S PRIVACY LAW.

The global nature of the Internet presents challenges for companies that must comply with children's data protection requirements across many jurisdictions, and for users who rely on global networks to access content and participate online. An anticipated benefit of the metaverse is its ability to enable access to experiences, people, resources, and markets around the world. However, organizations operating across geographies and jurisdictions face the complexities of meeting diverse and often conflicting legal requirements, particularly in the case of the age of consent to the collection of children's data and when the consent of a parent or legal guardian is needed.[90] These challenges exist in the context of other concerns and regulatory frameworks related to their safety, mental health, and access to appropriate experiences as they participate in digital environments.

Concerns about children's privacy and risks related to children's activity online have drawn the attention of governments and international organizations. Publication of the UK ICO's *Age-Appropriate Design Code*,[91] the Irish Data Protection Commissioner's *Children Front and Centre: Fundamentals for a Child-Oriented Approach to Data Processing*,[92] the French CNIL's *The Digital Rights of Children*,[93] and guidance issued by data protection authorities across Europe and in Asia highlight the importance policymakers and regulators place on children's privacy and the need to protect children online.[94]

Efforts to meet obligations to protect children's privacy will be further challenged by the need to comply with laws and guidance designed to protect other aspects of children's experiences in digital spaces. Standards bodies[95] and international organizations,[96] including the OECD,[97] have proposed instruments that address children's privacy and their rights and experiences in the digital environment. Companies in some cases will need to demonstrate how they mitigate the risks and potential harms data collection and processing in the metaverse will raise for children using child rights impact assessments.

Moreover, providing enhanced protections for children in many cases involves determining whether a child has reached the age of consent to data collection and processing. Age verification or estimation also may be necessary to determine whether a child should be allowed to enter to certain online spaces or engage in online activities. Because the tools used to make these determinations rely on gathering data about children, they also can raise significant privacy concerns.

08 BECAUSE THE CREATION AND FUNCTION OF THE METAVERSE WILL RELY EXTENSIVELY ON AI, IT MAY MIRROR – AND POSSIBLY INTENSIFY - THE CONCERNS AI RAISES, PARTICULARLY WITH RESPECT TO FAIRNESS, BIAS AND DISCRIMINATION IN AUTOMATED DECISION-MAKING OR PROFILING.

Concerns about issues of bias and discrimination that AI may raise are evident in the extensive resources that government, NGOs – including the OECD[98] - and businesses are investing to develop AI governance guidance that would address this risk. Implementers of AI in the metaverse will need to confront these questions when personal information is used to yield automated decisions about individuals and their experiences in the metaverse.

Bias may be introduced in AI in several ways. AI modelling may either intentionally introduce bias or inadvertently fail to mitigate or compensate for it. How AI is trained may also result in bias – if datasets are used that reflect existing prejudices or misrepresent the characteristics of different populations, algorithms likely will learn to make biased decisions. Bias also can occur when an AI algorithm is used in a situation for which it was not intended. AI's role in the creation of metaverse experiences raises the risk of discrimination that may result from bias; the extensive reliance on AI in the metaverse may compound this risk.

09 THE METAVERSE MAY PRESENT RISKS TO PRIVACY AND RESULTING HARMS THAT CANNOT CURRENTLY BE FORESEEN.

Because the metaverse is in its early stages, the privacy risks it may pose cannot fully be understood. As new immersive environments are created and linked, and as new applications are discovered and developed, existing privacy laws, regulations and guidance will continue to be tested. It will be important to monitor the evolution of the metaverse and the user's experience to assess and, as necessary, enhance the effectiveness and workability of data governance and privacy protections.

VII. RELEVANCE OF THE OECD PRIVACY **GUIDELINES IN THE METAVERSE**

The OECD Privacy Guidelines serve as one of the oldest, most foundational data protection and privacy governance instruments. They form the basis of protections that build trust across the digital marketplace, and of international guidance that fosters safe, robust transborder data flows. Published in 1980, they have informed law, regulation, and best practices across jurisdictions and industry sectors during a period of rapid technological change. The Guidelines were developed in response to the shared interest of OECD member countries in protecting privacy and promoting the movement of data across borders; they reflect the diverse views and perspectives of countries around the globe. The Guidelines can serve as a key tool in establishing and enhancing trust in the digital environment at a time when trust in technology is challenged.[99]

For over forty years the Guidelines have exerted real world, practical influence on development of technologies, data protection best practices, codes of conduct, laws, and regulations.[100] The eight basic principles are concise, technology-neutral, non-binding, and written in clear, commonly understood language.[101] As a result, they have proven adaptable to variations in governments and legal structures and have exerted enduring influence. Because the Guidelines center on data and data flows rather than any specific technology or application, they also have proven adaptable over a long period of rapid, dynamic developments in technologies, data processing methods and applications, and data-driven business models. Today they are available to apply to the development and deployment of the metaverse both for stakeholders who build it and governments and businesses seeking to design governance for it.[102] Because they inform existing laws, regulations, and best practices, the Guidelines already influence how the metaverse is built.

CROSS-BORDER PRIVACY RULES: A POTENTIAL MODEL FOR METAVERSE GOVERNANCE

The Cross-border Privacy Rules (CBPRs) that guide the implementation and oversight of the APEC Privacy Framework (the Framework) may offer an approach to metaverse governance that can work effectively across jurisdictions.

The Framework is a set of principles and implementation guidelines created to establish effective privacy protections while lowering barriers to information flows. The goal of Framework is to promote uninterrupted trade and economic growth in the Asia Pacific Economic Cooperation region of 21 countries.

The Framework reflects each of the principles found in the OECD Guidelines, however, it also includes the "Preventing Harm" principle. This principle requires that privacy protections, including self-regulatory efforts, education and awareness campaigns, laws, regulations, and enforcement mechanisms, are designed to prevent harm to individuals that is the result of wrongful collection and misuse of their personal information.

The Framework also emphasizes the principle of Accountability found in the OECD Guidelines. It recognizes that efficient and cost-effective business models often require data transfers between different types of organizations in different geographic locations and jurisdictions. The nature of the relationships between these organizations may vary, and the approaches to governance in their respective jurisdictions may differ with respect to legal tradition, requirements, and level of maturity. Therefore, the Framework encourages that when transferring data, organizations should be accountable for ensuring that the recipient will provide protections consistent with the principles of the Framework when it does not obtain consent to the transfer.

The creation of APEC Privacy Framework prompted the development of the APEC Cross-border Privacy Rules system. The CBPRs serve as an implementing system which requires participating businesses to develop and implement internal data privacy policies and practices consistent with the Framework. These policies and practices must be assessed as compliant with the minimum program requirements of the APEC CBPR system by an accountability agent and be enforceable by law.

The CBPR system also establishes a basis for certifying that an organization has implemented and abides by the nine principles of the APEC Privacy Framework. The CBPR system does not displace or change a country's domestic laws and regulations.

Where there are no applicable domestic privacy protection requirements in a country, the CBPR system is intended to provide a minimum level of protection. The privacy enforcement authorities of a country that participates in the system should have the ability to take enforcement actions when violations of the rules occur.

The APEC CBPRs break down the Framework principles into more granular requirements. Businesses must be able to demonstrate compliance with each of these requirements to obtain certification under the CBPR system. To make CBPRs work globally - as they would need to do to serve the metaverse - it will be necessary to understand how a global CBPR system can be coordinated with other international data protection requirements not based on the APEC Framework, such as those found in Latin American and South Asian countries. Because the CBPR system is not government led, it may be necessary to explore how requirements would be enforced in the context of the metaverse.

The Guidelines serve a harmonizing function.[103] Because they were drafted to be flexible and to promote interoperability between diverse data governance regimes, they are widely adopted as the basis not only for individual country laws,[104] but also to support regional governance systems.

The Guidelines form the elements of the U.S.-EU Privacy Framework, designed to support the legal transfer of data between the U.S. and the EU.[105] They can also be found in eight of the nine principles[106] of the APEC Privacy Framework and Cross-border Privacy Rules[107] system, an approach to trusted international data governance that provides for the protected movement of data across jurisdictions in the APEC region whose privacy regimes vary in their levels of maturity.

While the Guidelines have proven adaptable and enduring, the OECD has twice determined that their review was appropriate. They were revised in 2013 to address changes in the digital economy; the growing promise of innovation; and the increasing complexity of the digital environment, processing methods and business models.[108] This update stressed the Guidelines' orientation to risk assessment and mitigation and the need for proportionality in decisions about data uses and protections.[109] The updated Guidelines incorporated a new section that emphasized Accountability – the principle that holds organizations responsible for complying with measures which give effect to the Guidelines in their entirety - as a scalable tool that encouraged companies to embed privacy protections and practices into systems, technologies, and applications.[110]

The 2013 release also promoted a proportional, risk-based, outcomes-oriented approach to governance, and stressed implementation of privacy by design and privacy-enhancing technologies.[111]

A further review conducted in 2020-2021 did not result in changes to the Guidelines. Reviewers determined that their technology-neutral, principles-based approach continued to provide a strong foundation for governance.[112] The review did provide, however, supplementary commentary to further clarify the principle of Accountability[113] and the role of regulatory tools such as sandboxes.[114] It also raised questions about whether additional data subject rights – such as the right to data portability - might be appropriate, and highlighted the need for data enforcement authorities.

Finally, while recognizing the importance of the Guidelines themselves, it is important to consider them in the context of the broad portfolio of work relevant to the issue of privacy in the metaverse that has been undertaken by the OECD. This work provides further analysis of governance questions in more specific detail. Moreover, the OECD has issued Council Recommendations focused on questions relevant to this Project, among them digital security, electronic authentication, children's safety, connectivity, and artificial intelligence.[115]

As the evolution of the metaverse advances, the Guidelines can be relevant to promoting trusted governance in the following ways:

BECAUSE OF THEIR BROAD CROSS-SECTORAL ADOPTION, THE GUIDELINES CAN PROMOTE THE ACCOUNTABLE SHARING OF DATA ACROSS PLATFORMS, TECHNOLOGIES, AND COMPANIES NECESSARY TO FACILITATING INTEROPERABILITY.

Building and operating the metaverse will involve collaboration among companies and users across a range of platforms and technologies. To realize its full potential, users will need to be able to move between the environments that make up the metaverse and, through their avatar, carry with them their digital identities and assets. Data sharing will be critical to making this movement between digital spaces possible. The Guidelines have served as the basis for data protection and governance within companies across industry sectors . As established principles that protect privacy and facilitate the movement of data, they create a common structure for governance grounded in broadly recognized protections. This expectation that certain principles guide data governance across entities in the metaverse can promote the interoperability between platforms, technologies, and ultimately digital spaces necessary to optimize the evolving metaverse experience and promote innovation.

THE GUIDELINES OFFER A FOUNDATION FOR REGULATORY COHERENCE.

The global development and deployment of the metaverse and the need for protected, robust data flows highlight the importance of harmonized approaches to governance and the need for regulatory coherence. The cross-jurisdictional nature of the metaverse will reinforce existing data protection policy challenges that are inherently international, and solutions will require enhanced cross-border cooperation. Many companies operating in the metaverse will need overarching global data governance to operationalize and scale consistent, efficient protections while also complying with national laws.

The Guidelines have proven to support governance that works effectively across jurisdictions whose legal systems may vary and whose data protection regimes may differ in their level of maturity. The development and implementation of the APEC Privacy Framework and Cross-border Privacy system – an approach primarily based on the Guidelines' underlying principles – serves as an example of how the Guidelines can promote the harmonized governance needed as the metaverse becomes an increasingly borderless and globally shared space. The Guidelines may also encourage a more unified approach across industry best practices and standards development that accommodates the requirements of various technologies, applications and business models.

BECAUSE THE GUIDELINES FOCUS ON DATA AND NOT ON ANY SPECIFIC TECHNOLOGY, THEY ARE WELL SUITED TO SUPPORT GOVERNANCE IN THE METAVERSE - AN ENVIRONMENT THAT WILL COMPRISE DIVERSE TECHNOLOGIES, PLATFORMS, AND DATA PROCESSING METHODS.

The technology-neutral character of the guidelines makes them particularly suited to advancing coherent governance in the metaverse. To establish and maintain user trust, privacy governance will need to work effectively across the wide variety of systems and entities that facilitate the environment. The Guidelines' focus on data rather than on any single application or technology enables their utility as a data governance tool across the diverse technologies, platforms, and data processing methods that will make up the metaverse. Their technology-neutral, data-centered design may position them as "future-proof" policy governance as the metaverse continues to evolve and as the innovations that enable its growth and refinement emerge.

BECAUSE THE GUIDELINES DRAW NO DISTINCTION BETWEEN CONTROLLERS AND PROCESSORS, THEY MAY BE MORE EASILY AND EFFECTIVELY APPLIED IN THE METAVERSE.

The Guidelines establish principles to govern the collection and processing of data, and the rights (*e.g.*, the right to access, correct and amend their personal data) of individuals in their data. But they do not designate which parties are responsible for abiding by the principles or honoring those rights. By contrast, laws such as the EU's General Data Protection Regulation[117] (and legislation around the world modelled on the GDPR) impose specific obligations on entities based on their role as either a controller of data or a processor.[118] The complex network of relationships between companies, platforms, and participants in the metaverse could create an environment in which the controller and processor roles may coincide or change depending on the application, user, or activity. Attempting to distinguish controllers and processors may become cumbersome without necessarily furthering the goal of privacy.

By establishing principles that apply regardless of controller/processor status, the Guidelines can promote flexible allocation of responsibility for risk assessment and mitigation, so that solutions can be implemented where they are most needed and optimally effective. Foregoing this distinction may also facilitate innovative approaches to applying the Guidelines, *e.g.*, the creation of chains of accountability, that will promote an environment conducive to trusted data use and sharing in the metaverse. This flexibility could also enable new thinking about how data protection and privacy regulators will supervise, investigate, enforce compliance, and provide guidance in the metaverse.

THE GUIDELINES' PRINCIPLE OF ACCOUNTABILITY MAY OFFER ELEMENTS OF A WORKABLE APPROACH TO PRIVACY GOVERNANCE IN THE METAVERSE.

The focus on the principle of Accountability in the 2013 and 2021 reviews – particularly the emphasis placed on risk and proportionality and the need to provide protections while encouraging responsible innovation - will be important in discussions of governance in the metaverse. The principle obligates organizations be accountable for complying with measures which give effect to all of the OECD Privacy Principles. Significantly, the guidance provided by the OECD about the implementation of the Accountability principle reflects an approach to meeting that obligation in a way that considers both the risks of processing and the potential benefits it may offer. It accommodates the complexity of data collection and processing methods, emerging technologies, and dynamic business models. It encourages the application of privacy by design – the practice of building measures into a technology, process, service, or product that foster privacy as a default.[119]

Accountability may be particularly suited to address privacy in the metaverse. However, while Accountability is referenced in the GDPR and is incorporated into emerging laws and guidance, there has been a lack of focus on the central role it can play in data protection, particularly in complex environments such as the metaverse where the effectiveness of principles and safeguards such as transparency and user choice will need to be carefully considered. While user awareness and control remain important tools and can evolve further in the metaverse by applying user experience design approaches, by placing on companies the responsibility for data protection and privacy-respectful collection, Accountability creates the opportunity for balanced, proportionate and context-specific roles for companies and users in highly complex data environments.

BECAUSE THEY ARE WIDELY RECOGNIZED AND ADOPTED, AND DEVELOPED WITH THE INPUT OF RELEVANT STAKEHOLDERS, THE GUIDELINES CAN SUPPORT MULTISTAKEHOLDER SOLUTIONS.

The OECD Guidelines form the foundation not only of individual country laws and international agreements - they also reflect and form the basis of privacy guidance and best practices within companies across industry sectors. They can serve as a workable starting point for privacy solutions in the metaverse, which will require collaboration and adoption by governments, businesses, developers, and individuals.

HIGHLIGHTS OF RELEVANT OECD AND *BUSINESS AT OECD* INITIATIVES

Business at OECD's project on Privacy, Immersive Technologies, and the Metaverse aims to contribute to related work undertaken by the OECD. It also builds on other *Business at OECD* initiatives centered on relevant technologies and issues.

OECD GLOBAL FORUM ON TECHNOLOGY (GFT)

Deep Dive on Immersive Technology

The OECD Global Forum on Technology (GFT) in early 2023 released a policy brief, "Technology Deep Dive: Immersive Technology," as background for the GFT's 6 June 2023 inaugural event. The brief provides essential information about immersive technologies; reviews anticipated applications and benefits; and suggests some potential policy implications.

The brief introduces a consideration of users' experiences with immersive technology; the trajectory of the technology's development across industry sectors; its potential to offer solutions to societal and environmental issues; and the risks it may raise. It highlights the access immersive technology may afford individuals to a broad range of experiences and the possibility that these may be unevenly distributed and available among users. Finally, the brief proposes questions for further consideration, including how policy can promote benefits and mitigate risks.

Convening Stakeholder Discussions – Kyoto

At the October 2023 Internet Governance Forum in Kyoto, the Government of Japan and the GFT organized a discussion on immersive technologies, in which participants identified risks and policy challenges of immersive technologies. The discussion highlighted the collection and processing of personal data – imcluding biomedical data and data that reveals an individual's emotional state – required by these technologies. It also considered the potential effects of immersive technologies and the collection of this kind of data on privacy, security, and online safety.

The discussion noted the OECD Privacy Guidelines' continued relevance as a tool for data governance in immersive technologies, but raised questions related to their implementation. It also highlighted that the cross-jurisdictional nature of the metaverse raises policy challenges that are inherently international, and that governance solutions will require enhanced cross-border and cross-sectoral cooperation.[120]

OECD Digital Economy Outlook 2024

In May 2024 the OECD released Volume I of a two-part Digital Economy Outlook 2024 (DEO). In a chapter titled "The Future of Immersive Technologies,"[121] the DEO raises questions related to safety and protection of user rights in immersive environments, and considerations related to security and individual privacy. The DEO also highlights how negative behaviors in online and immersive environments affect mental health, and proposes a policy agenda aimed at promoting solutions and opportunities to minimise potential risks raised in immersive environments.[122]

BUSINESS AT OECD DIGITAL POLICY COMMITTEE

"Implementing OECD AI Principles: Challenges and Best Practices"

In 2022 *Business at OECD*'s Digital Policy Committee released work on the trustworthy implementation of artificial intelligence, a critical building block of immersive technologies and the metaverse. Its paper on "Implementing OECD AI principles: Challenges and Best Practices"[123] highlights business's role in the transition towards trustworthy AI technologies, and explores through practical examples companies' efforts to effectively embed trustworthy AI within their organizations. It also features recommendations for governments designed to foster a positive environment for development and adoption of trustworthy AI.

VIII. DESIGNING FOR PRIVACY IN THE **METAVERSE**

Because the metaverse is in its early stages, developers are positioned to identify at the outset an address at the outset the privacy concerns it may raise, to make privacy-enhancing design decisions and to integrate effective solutions. The benefits of "building in" data governance and privacy solutions through privacy by design and privacy enhancing technologies (PETs) are well recognized.

PRIVACY BY DESIGN

Privacy by design is an approach to technology design and implementation that integrates privacy into the creation and operation of new devices, IT systems, networked infrastructure, and company policies.[124] Developers identify potential privacy problems and data protection compliance obligations at the earliest stages of design and development, and based on this analysis, integrate and test privacy solutions as work advances and an offering, policy, or process is launched.[125]

Developing and integrating privacy solutions in the early phases of a project makes it possible to set controls and defaults in such a way that laws, regulations, and guidance obligations are met. It provides the best opportunity to make decisions about how to reconcile competing privacy demands and build appropriate responses to requirements into systems and policies. Designing privacy solutions and building them into new products and services at the beginning of the design process is recognized to result in enhanced privacy outcomes.[126]

Implementation of privacy by design involves choices related both to business decisions about data collection and processing and to implementing technological controls. Designing privacy into business models involves making choices about what data is necessary to create and deliver a product, service, or experience; how that data will be processed; what inferences are and are not necessary for innovation and personalization; and when and under what circumstances commercialization of the data collected and derived is appropriate. Even before technical privacy controls are identified and implemented, choices related to business model design are often instrumental in implementing privacy protections and pro-privacy defaults.

PRIVACY ENHANCING TECHNOLOGIES

Privacy-enhancing technologies (PETs) may serve as a tool in implementing privacy by design in the metaverse.[127] They may not, on their own, address all privacy concerns and data protection obligations. However, when the appropriate PETs correspond to the level of risk posed, they provide mechanisms that could lessen the user's burden of policing privacy *and* preserve the quality of the metaverse experience.

Zero-knowledge proofs (ZKPs), for example, make it possible to authenticate information and verify the validity of information without revealing sensitive personal details. This technology enables users to explore, transact and create in the metaverse without revealing their identities.[128] Such tools can serve an important role in facilitating identity management, user transition across services, and interoperability while maintaining data minimization. Decentralized identity systems enable users to control their identities and personal data and limit the involvement of a centralized identity authority in authentication and validation. Using blockchain technology and cryptographic algorithms, these systems ensure that users maintain ownership and control over their digital personas in virtual environments.[129] Pseudonymization and anonymization measures, including solutions such as differential privacy or the use of synthetic data, also enable users to protect their identity in the metaverse.[130]

Google's Federated Learning tool enables mobile phones to collaboratively learn a shared prediction model while keeping all the training data on the device, so that it is not necessary to store data in the cloud in order to conduct machine learning.[131] PETs also can facilitate user choices about secondary uses of data[132] by serving as intermediaries such as data trusts. By providing controls and tools to minimize how much data is shared, intermediaries can facilitate and manage user choices across a range of platforms. Data trusts also can facilitate anonymisation and pseudonymisation of user data.

TRUSTED IDENTITY IN THE METAVERSE

To realize the metaverse's full potential, it will be important that participants in the environment – individual users, businesses, institutions, financial services companies, and governments - can trust institutions, transactions, and each other. Creating that trust requires the secure verification and authentication of users. Establishing that users are who they represent themselves to be and meet the requisite criteria to make a purchase, enter an immersive space, access certain services (such as health care or education), or engage in a metaverse activity will enhance trust in the metaverse environment and experience.

Industry and government are challenged to develop and deploy identity tools that provide the necessary assurances across the metaverse while respecting the privacy of individuals. Activity in the metaverse will be observed by more entities and will involve the collection of more data than occurs in the existing digital environment. It will be important to understand what entities collect this data, what data is necessary for entities supplying trust services to perform their designated functions, and with whom the data is appropriately shared.[133] It will also be important to consider flexibility among solutions so that the level of verification and the nature of the authentication - and therefore the amount and kind of data required to reliably accomplish these functions - corresponds to the sensitivity and the risk posed by various kinds of transactions. Because the metaverse will enable individuals to move across platforms and between environments and experiences, it also be necessary to determine whether, and in what instances, identity may be ported across applications.

Developing effective, privacy-respectful identity management solutions will be critical to the success of the metaverse. Acceptance of such solutions across platforms and services is also key. The nature of potential solutions could vary. Whether identity management is best served by a single, global identity system that is interoperable across platforms, or whether a system that accommodates multiple identities to maintain privacy and security is preferable is the subject of ongoing debate.[134]

Organizations have recognized several incentives for adoption of PETs:

I. PETs FACILITATE COMPLIANCE

PETs can support data use that adheres to data protection principles and complies with law and regulation. By operationalizing and embedding core privacy principles and legal requirements into technology choices core privacy principles,[135] PETs can promote organizations' ability to meet their privacy obligations without sacrificing performance or the user experience. PETs also can be implemented to mitigate risks that are identified in a data protection or privacy impact assessment.

II. PETs RAISE AN ORGANIZATION'S ACCOUNTABILITY PROFILE

By facilitating implementation of privacy-protecting data practices, PETs can also serve as a significant tool in establishing organizations' accountability and responsible data practices. Companies increasingly recognize that accountable data practices - particularly in complex data and technology environments like the metaverse - are fundamental to fostering the trust of consumers. Organizations that can demonstrate their accountability also position themselves for business opportunities, partnerships, and investment. Certified PETs also may offer an additional way to demonstrate accountability.

III. PETs ENABLE COMPANIES TO PROTECT PRIVACY IN THE FACE OF CHANGES IN DATA PROCESSING METHODS

PETs can serve as a tool to protect privacy as technologies and processing methods evolve. Where emerging technologies have enabled new uses of customer data, PETs have permitted organizations to reap the benefits of new processing without sacrificing consumer privacy.[136]

IV. PETs FACILITATE PROTECTED DATA SHARING

PETs can enable protected data sharing among different teams within organizations and with third-party vendors. Such sharing may be especially useful in the metaverse, where data sharing across platforms, technologies and companies will be essential to the ability to create virtual experiences.

V. PETs ENHANCE DATA SECURITY

PETs are recognized by data security experts to mitigate the risk of security breach. Because PETs render data unintelligible, hackers are not able to link individuals to their data.[137]

Privacy by design will be important to creating a metaverse that provides effective data protection. Because the metaverse is in its early stages, the opportunity exists to implement privacy principles into its design at the earliest stages of its development. In doing so, it will be important not to consider individual principles in isolation. Privacy by design presents encourages developers to consider privacy in light of regulatory and design requirements intended to address other online issues, e.g., integrating measures to ensure an age appropriate, protected experience for children; providing tools for users with disabilities or limited literacy; and equipping users with practical measures to enhance their safety. Whereas a compliance checklist will not lead to optimal privacy design outcomes, design principles that allow for bespoke solutions will. To be credible, privacy by design in the metaverse will require follow-up that includes ongoing monitoring to ensure that the measures taken effectively promote privacy. It will also be important to consider whether existing guidance regarding the use of PETs can be applied effectively in the metaverse or whether new guidance will be needed.

IX. EFFORTS TO DEVELOP GUIDANCE FOR **PRIVACY IN THE METAVERSE**

Confidence in the metaverse's potential is evident in the initiatives NGOs, standards bodies and trade associations already have undertaken to understand and address issues of privacy in the metaverse. These efforts also reflect the recognition that early development and adoption of solutions will enhance the ability to build a metaverse that is privacy-respectful and that encourages innovation.

XR ASSOCIATION'S "BASIC BELIEFS"

The XR Association is a consortium of companies that represents the broad ecosystem of the XR industry, including headset manufacturers, technology platforms, component and peripheral companies, internet infrastructure companies, enterprise solution providers, and corporate end-users. The Association's "Basic Beliefs" urge manufacturers to incorporate privacy by design in their development processes so that privacy protection is the default for XR devices. They promote transparency and user control over the collection and sharing data during the XR experience. The "Basic Beliefs" also highlight the privacy interests of bystanders in the metaverse. Finally, they emphasize that protecting children should be a top priority for developers, but also that parents must play a role in protecting their children and should have available the information they need to support their children's positive XR experience.[142]

FUTURE OF PRIVACY FORUM GUIDELINES

The Future of Privacy Forum (FPF)[149] is non-profit industry organization that advances privacy leadership, scholarship, and data practices in support of emerging technologies. FPF has developed guidelines designed to promote the benefits and mitigate the risks of emerging XR technology.[150]

The guidelines focus on establishing clear policies regarding collection, processing and sharing of sensitive XR data, limiting third party access, user consent, and steps to automatically aggregate or pseudonymize it. They also rely on accountability "feedback loops" to be sure organizations hear the concerns of experts and users. The guidelines encourage empowerment of XR users through privacy-protective default settings and user controls. Finally, they encourage XR developers to consult with stakeholders and to integrate responses to their concerns into future design decisions.[151]

THE WORK OF STANDARDS ORGANIZATIONS

X Reality Safety Intelligence Framework

X Reality Safety Intelligence (XRSI), a global, non-profit standards development organization brings together a global network of experts to provide intelligence and advisory services vital for the protection and positive experience of users in emerging technology ecosystems. The organization applies its expertise to addressing such concerns as safety, privacy, human rights, human wellbeing, responsible innovation, governance, and regulation.

XRSI's Privacy and Safety Framework is a free, globally accessible baseline rulebook built by experts from diverse backgrounds and domains. The framework sets baseline standards, guidelines, and best practices.

It incorporates privacy requirements drawn from the EU's GDPR, The U.S. National Institute of Standards and Technology (NIST) guidance, the U.S. Family Educational Rights and Privacy Act (FERPA), the U.S. Children's Online Privacy Protection Rule (COPPA), and other evolving laws. The framework is designed to adapt and incorporate additional requirements as new regulations come into effect.

The framework establishes privacy by design guidance and expands the definition of personal information to include data inferred from biometrics. It also highlights the data subject's right to know what data about them is collected, how it is used, and how it is shared.[143]

The Metaverse Standards Forum

The Metaverse Standards Forum, a cooperative organization comprising leading standards organizations and companies, is committed to development of interoperable standards for privacy, cybersecurity, and identity the metaverse. Recognizing that interoperability is essential to implementation of the metaverse, the forum seeks solutions that will enhance the ability of multiple technologies to work together. It also attempts to build bridges between applications and to create a platform that is open and inclusive.[144]

IEEE Global Initiative on Ethics in Extended Reality/ P7030 Global XR Ethics Standard Working Group

IEEE Global Initiative on Ethics in Extended Reality's develops white papers, workshops, policies, and standards with the goal of purposeful implementation of Extended Reality technologies. [145]

IEEE's P7030 Global Ethics Standard Working Group has developed a "Recommended Practice for Ethical Assessment of Extended Reality (XR) Technologies." The standard establishes uniform set of definitions, and a methodology to assess relevant social and technical considerations and practices related to XR[146] with the goal of furthering the positive design of XR systems.[147] The standard also provides a high-level overview of the technical and "socio-technical" aspects of XR; XR definitions and classifications; a standardized definition of ethical assessment methodologies for XR products, services and systems; and a high-level ethical assessment methodology for the design of XR products, services and systems.[148]

X. CONCLUSION AND **RECOMMENDATIONS**

The consultations and research conducted in this Project highlight the relevance of the OECD Privacy Guidelines as a framework for privacy governance in the metaverse. Their principles-based approach, global acceptance, and proven effectiveness make them particularly suited to addressing the complexities of the metaverse environment. Critically, the Guidelines have proven adaptable over decades of rapid technological change. This flexibility will be necessary to any approach to privacy protection in the metaverse, whose development will rely on innovations in technology and data processing.

The Project reveals that the metaverse presents several unprecedented challenges related to the scale and scope of the data collected and used. However, some of these are extensions of existing governance challenges such as those that arise in digital identity management for financial services and data processing via smart phones. The lessons learned through efforts to address these issues – particularly as they relate to interoperability and data portability - can inform the development of privacy solutions in the metaverse. Similarly, the metaverse will depend significantly on the extensive deployment of AI. Existing guidance related to privacy in AI, *e.g.*, on AI model development and data minimization, should be considered in the context of the application of the Guidelines in the metaverse.

The Project also makes clear that application of the Guidelines in accordance with current norms is challenged in the metaverse. While transparency, for example, will always serve as a key baseline component of governance, further exploration is needed to consider when consent and user control are necessary and effective and when other alternative compliance mechanisms, such as legitimate interests, should be implemented to reduce risk and protect individuals.

The need to resolve these tensions argues for the role of the principle of Accountability in metaverse privacy governance. Accountability requires organizations to comply with measures that give effect to *all* of the Guidelines' principles. In doing so, it supports responsible innovation, users' rights, and mitigation of privacy risks. Privacy by design and PETs, essential to the implementation of Accountability, will play a critical role in the metaverse. In the case of transparency, data minimization, and other instances where tensions exist between the evolution of the metaverse and the practical application of the Guidelines, privacy by design and PETs can help mitigate risk. Deeper exploration of the outcomes-based Accountability approach to governance that accounts for the metaverse's complexity could enable the Guideline's long-term relevance.

Thus, while the Guidelines remain highly relevant, how their application can continue to support privacy and responsible innovation in the metaverse merits exploration. While it may not be necessary to update the Guidelines to promote their effectiveness, more clarity about how they may be applied to address the issues highlighted in this report may be needed. Case studies or an additional explanatory memorandum that sits below the Guidelines could provide such clarity. Considering questions of privacy now, while development of the metaverse is in its early stages, presents an opportunity to position the Guidelines to support and promote robust innovation and provide essential privacy critical for user trust.

RECOMMENDATIONS

The OECD Privacy Guidelines continue to serve as foundational guidance for privacy and a widely adopted approach to protections that serve an increasingly complex digital environment. We recommend that the OECD Digital Policy Committee, as the leading convenor of multistakeholder dialogues and developer of consensus-based responses to digital policy issues and challenges, advance the following:

01

Deepen and broaden the evidence base regarding the relevance and applicability of the OECD Guidelines in the metaverse by delivering practical case studies and multi-stakeholder led research.

02

Map OECD instruments, reports, and ongoing work relevant to pri-vacy in the metaverse, including initiatives related to AI, international data transfers, children, data sharing and data portability. The work of the OECD Expert Group on AI, Data and Privacy will be especially relevant in this regard.

03

Consider the role of regulatory sandboxes and their possible utility in understanding the strengths and limitations of the Guidelines as an oversight and policy development tool. Provide relevant OECD policy analysis and support for data protection authority-hosted, pilot sandboxes focused on regulation in the metaverse. Consider how sandboxes could be designed to include multiple participants to understand their role in a digital eco-system that involves a range of users, platforms, technologies, and the movement of data across jurisdictions.

04

To ensure adequate consideration of the principle of Accountability and its role in effective data governance, consider whether its workable deployment in the meta-verse could benefit from additional recommendations to complement existing guidance.

05

Explore how privacy enhancing technologies and privacy by design can be deployed to facilitate privacy in the metaverse. Identify ways in which the OECD Guidelines, particularly the principle of accountability, can support their implementation, effectiveness, and ability to mitigate risk and enhance individuals' privacy.[152]

APPENDIX - **USE CASES**

INGKA GROUP
An IKEA retailer

As housing costs rise and the availability of housing shrinks, fewer people can readily transition to larger living spaces. Increasingly people live longer in smaller, more compact spaces that must accommodate more possessions and serve a myriad of purposes. They seek to optimize their existing spaces to make them work better for them at all stages of life - to create homes that reflect the way they live, and that serve both their current needs and anticipate future life changes. At the same time, they must make the most of their budgets and limit future renovation costs.

IKEA's *life-changing home staging* is an XR/AI-enabled immersive experience that promotes future-proof home design. In an engaging environment that encourages exploration, customers experiment with their vision for their living spaces and plan for what their homes may look like at different stages of their lives, taking into consideration planned-for milestones and the demands of unexpected life events. They visualise, share, and experience their ideas in a lifelike environment to confidently make decisions about creating comfortable, functional, and sustainable living spaces. IKEA's home staging empowers them to make the best possible use of their living space as currently configured and to anticipate future life changes. One aspect of this tool is a *life stage prediction* feature that allows customers to submit information about their aspirations and pursuits such as children, hobbies, and potential career paths.

It processes that information to create an immersive visualization of how their living spaces can be adapted to accommodate and support the future they envision. The feature, for example, enables the customer to experience how their existing space may be reconfigured to incorporate a nursery or a home office.

The tool's *scenario builder* shows customers how their current living space may evolve over time. Using their existing home furnishings as a starting point, it suggests potential additions, replacements, and modifications. It can display images of their "future memories" – pictures of milestone still to be reached, such as birthdays, weddings, and anniversaries – to be celebrated in these redesigned spaces.

Finally, these solutions also take into consideration the financial aspects of creating and maintaining a supportive living space. When looking for new interior design solutions, people search for the best value for money spent. This immersive/3D-enabled environment not only makes it possible for people to integrate designs for their living space across all stages of life and to experiment with how they might evolve – it also helps them strategize and plan for how these changes will be paid for.

By empowering customers to imagine and plan their current and future living spaces, immersive technologies can democratise interior design, making it more accessible and affordable. Immersive technologies can ensure that - regardless of social and economic constraints - customers have the resources necessary to access and create healthy, functional, and sustainable living spaces.

The LEGO Group is working to ensure that respect for children's rights and positive online experiences are integrated into the design not only of LEGO's offerings but of the next generation of the internet. The advent of the metaverse provides an opportunity to benefit from the lessons of the first-generation internet - a digital environment that was not designed with children's best interests in mind, and where intrusive data collection practices, complex terms and conditions, manipulative design and a lack of safeguards often resulted in online environments that exposed children to harm and exploitation. LEGO believes that this new phase in the evolution of the digital experience represents a critical opportunity to create immersive, virtual spaces that foster the wellbeing of children.

To this end, the LEGO Group has co-founded a research initiative with UNICEF called Responsible Innovation in Technology for Children (RITEC) which seeks to (1) understand the elements of child wellbeing in a digital era – e.g., creativity, social connection, emotional regulation, and safety, and (2) equip the LEGO Group and other businesses with tools to design positive, constructive experiences for children. This commitment to children's wellbeing online is central to how the LEGO Group envisions the virtual worlds and web interoperability that are the future of the internet. The LEGO Group believes that children have a right to access online spaces that are equipped with strong privacy and safety protections and that empower them to explore and make age-appropriate choices.

A joint initiative of Epic Games and the LEGO Group centres on these aspects of children's digital experience. Both companies are committed to building a metaverse that:

- protects children's right to play by making safety and wellbeing a priority;

- safeguards children's privacy by putting their best interests first; and

- empowers children and adults with tools that give them control over their digital experience.

In December 2023, this partnership released LEGO Fortnite, the first of many collaborative offerings. This standalone game, embedded within the wider Fortnite ecosystem, enables children to build, create, and play with friends in a world made of LEGO Bricks. It includes stronger protections for younger audiences, age-appropriate messaging, active con-tent moderation and robust player controls. Player experiences - including avatars and achievements - are linked across the Epic and LEGO ecosystems so that children enjoy a persistent presence within connected Fortnite and LEGO services. Among these is LEGO Insider's Club, which provides children with skill-building classes, trophies and a safe online community.

The LEGO Group sees this initiative as a first step toward a metaverse in which children can access not only individual, stand-alone experiences, but age-appropriate ecosystems where parents can be confident that their kids are playing, creating, and learning in an environment where diverse media are designed to put their safety and privacy first. To build these spaces, the LEGO Group believes service providers need first to commit to a wellbeing-by-design approach to development of their child-facing experiences, incorporating the lessons learned from RITEC. With this commitment as a foundation, collaboration between participating platforms to align on standards, policies, and service architecture will foster development of a metaverse that promotes the best interests of children of all ages.

Telefónica

Telefónica's Movistar Immersive Ex-perience is an app that enables users to enjoy an immersive experience as they shop, watch films, or participate in sports.

To address privacy issues, users may use the app in two alternative modes: the individual experience and the multiuser experience.

Users who choose the *individual experience* participate in the metaverse alone. In this mode, the user does not see or interact with other users. The user's data is segregated from that of others even when that data is present in the same immersive space. Users may be confident of their privacy when their immersive experience – such as shopping, banking or simply searching for metaverse activities or spaces - involves processing or generating sensitive data.

Users who engage in the *multiuser experience* interact with any user who may be in the same metaverse room or space. The app allows the user to switch off speakers so that some or all users in the space are not able to hear them. In the multiuser experience, information flows only between the user and the app – other users are prevented from seeing, hearing, or identifying the user's activity. Aura, Telefonica's digital assistant, enables users to manage their experience in Movistar using natural language and to limit who hears their conversations with the assistant or with a real-world caller.

By implementing principles of privacy by design and embedding protections into the technology, Telefónica offers an immersive experience that advances both innovation and respect for individual's rights, where users can participate knowing that their privacy is respected.

NEC

NEC's new business offering - training solutions that use immersive technologies to replicate specialized business-critical operations - includes training for first responders in crisis and disaster zones; flight attendants' management of in-flight and on-the-ground emergencies; and employees working on aseptic vaccine production processes. The benefits of these solutions include better training outcomes, dramatic reduction in investment in physical training facilities, scaling of skilled operation staffs, reduction in carbon emissions produced by training exercises, and enhanced openness and inclusivity in learning and employment opportunities. From a business perspective, immersive technologies afford a new opportunity to address Japan's societal challenges. As a result, virtualized professional training is becoming a near-term economic driver.

CASE-1: VR TRAINING OF CABIN ATTENDANTS

In 2019, NEC and All Nippon Airways (ANA) introduced the first case of VR -based training for inflight safety operations. The VR solution immerses personnel in in-flight emergency situations - such as an outbreak of fire in-flight or a sudden loss of cabin pressure - that are otherwise difficult to replicate for training purposes. It also provides guidance about how to conduct security checks of cabin equipment. After using NEC's VR-based training, ANA reported that (1) VR-based training of cabin attendants was more effective and better equipped personnel to take swift, appropriate action under rare emergency situations, and (2) cabin crews were better able to adopt appropriate procedures because of the opportunity VR afforded them to participate in repeated practice drills. Furthermore, the immediate experience of a virtual inflight fire or cabin decompression provided trainees with a better understanding of how errors can lead to serious emergencies. Moreover, even as outcomes improved, the VR experience reduced the resources required to onboard the 800 new trainees that join the company each year.

CASE-2: SAFETY FOR CONSTRUCTION WORKERS

NEC provides for the construction industry a variety of VR solutions designed to enhance employee education, reduce workplace accidents, and provide workers with a virtual construction site experience.

In virtually-replicated construction sites, workers collaborate using 3D models. Working together, employees efficiently identify in real time problems that may emerge on project sites and ways to address them. Workers trained in these virtual spaces are able not only to anticipate and prevent potential accidents but also to understand the critical importance of pre-project inspections.

Kanno Kensetsu, a Japan-based company that provides residential construction services, launched the "Danger Experience Practical Skill Center" facility with the goal of reducing on-site accidents. The VR experience of a landslide or other natural disaster, or of falling from high scaffolding has been found to raise employees' awareness of safety requirements and to improve safety outcomes. Noting these successes, companies in other industries and public authorities now visit the Center to participate in Kanno's VR training workshops, and in some cases have planned to provide similar training to personnel across their organizations.

CASE-3: VACCINE PRODUCTION

In 2019, NEC and Takeda Pharmaceuticals announced a VR-based aseptic operation training solution for vaccine manufacturing.

Currently, vaccine manufacturing processes accommodate various new technologies and automated procedures. However, in cases where delicate and careful operations are essential, manual labour is still required. In such instances, workers must be knowledgeable not only about the vaccines themselves, but also about the correct aseptic production protocols. Training in these protocols requires extensive education. Takeda Pharmaceuticals, for this reason, recognizes that efforts to secure and invest in workers who understand aseptic procedures and the time it takes to train them pose significant management challenges.

In VR training for aseptic production operations, various facilities and instruments used in aseptic rooms are reproduced in the virtual space where trainees experience and learn the protocols they must adhere to. More specifically, the solution isolates worker actions that pose high risk of introducing contaminants – such as contact between a worker and a production apparatus -- evaluating the position, angle and contact between a trainee's hand and the equipment in use. This VR training can detect 260 cases that violate 20 established requirements, identify the cause of contamination risk, and instruct trainees in how to address or avoid risky practices.

Once the aseptic room environment is recreated in virtual space, there are no limits on access to the facility and the time available for training. Also, skilled experts can objectively assess, based on empirical evidence, the effectiveness of the training.

The VR training addresses concerns about global sustainability by reducing waste produced by materials used in the aseptic training. It also supports a significantly less costly training solution. Prior to introduction of VR technology, training involved the use of expensive undiluted chemicals; every error that occurred in a training session resulted of costly waste. Synthesis of these chemicals is a dangerous process that generate harmful gases. By eliminating their use, VR training furthered NEC's goal to create a safe training environment for employees.

Technologies that create a sense of presence and shared space offer new ways for educators to engage and interact with students. They empower teachers with tools to do what they do best — teach. Placing these technologies in the hands of teachers so they can shape how they're used will be key to unlocking this potential. Meta wants more and more teachers and students to benefit from these technologies.

Immersive technologies, combined with powerful advances in Artificial Intelligence (AI), create opportunities for education experiences that are much more tailored to the needs of individual students. Using AI, a teacher with little technical experience can design a virtual environment to deliver a specific lesson. It will become possible to quickly and easily personalize curriculum materials to the learning needs of individual students. And because AI can process and translate multiple languages simultaneously, it can serve as a powerful tool for language learning, especially when combined with immersive technologies.

FOUR WAYS THE METAVERSE IS TRANSFORMING EDUCATION AND TRAINING

I. RE-IMAGINING SCHOOL LESSONS:

The metaverse can free teachers from the constraints of the classroom and make lessons so much more vivid and interactive for their students. In the metaverse, teachers can introduce students to marine biology on the ocean floor or deliver a philosophy lecture in an amphitheater in ancient Rome. Apps like Nano by Lighthaus Inc. deploy students as trainees in a top-secret bioresearch program that is fighting against an unknown virus. By controlling a nanodrone, a tiny machine that is injected into the human body, the trainee is immersed in a thrilling biology adventure with real science in its DNA.

II. BRINGING TEACHERS AND STUDENTS TOGETHER IN SHARED VIRTUAL SPACES:

The metaverse will bring classes, students, and teachers together regardless of geography in an immersive, realistic way. At Morehouse College in Atlanta, Georgia, biomolecular chemist Dr. Muhsinah Morris teaches her students in a virtual lab — a digital twin of the chemistry lab at the physical university. In the virtual lab, students conduct experiments just as they would if they were present in person.

III. ENHANCING VOCATIONAL TRAINING AND REMOVING RISK:

The metaverse can make vocational training more accessible and affordable. The metaverse will enable simulation of situations people will encounter in the workplace — particularly those where real world experience might be challenging or potentially dangerous. Plumbers can train on virtual pipes; firefighters can escape virtual buildings; nurses can train on virtual patients. Interplay Learning offers VR training for small and medium sized businesses, enterprises, & individuals in HVAC, plumbing, electrical, solar & facilities maintenance. Through VR, skilled tradespersons can safely practice diagnostic and troubleshooting skills on life-like equipment in a variety of industries.

IV. NEW OPPORTUNITIES FOR LIFELONG LEARNING:

One of the most common misunderstandings about the metaverse is that it is only relevant to online gaming. While gaming has played a significant role in the evolution of these technologies thus far, it represents only one part of the experience. Many Meta Quest users see education as one of the main motivations for owning their device, in addition to health and wellbeing, work, fitness, and socializing.

KEY TAKEAWAYS:

While these technologies are still in their early stages, promising signs of their potential impact in education are evident. A recent report by PwC found that 40% of VR learners are more confident in applying what they've been taught, and 150% more engaged during classes. The XR Association (XRA) and the International Society for Technology in Education (ISTE) found that 77% of educators believe immersive technologies ignite curiosity and improve engagement in class.

In a randomized control study of the VR mathematics program Prisms, students learning in VR had test scored 11% higher than those in the control group. The study also identified an increase in students' confidence, engagement, and ability to describe mathematical concepts. Morehouse College in Atlanta, Georgia, which has been an early adopter of VR, found that students who learned in VR had an average final test score of 85, versus 78 in person and 81 for traditional online methods. They also found an uplift in student attendance and engagement.

REFERENCES

[1]In this report, we use the term "metaverse" to include both the metaverse and relevant immersive technologies that are the subject of this Project.

[2]As the platform for users' digital experience has evolved from mainframes to personal computers to mobile computing, users' experience of the Internet also has progressed from text to images to video. The immersive, three-dimensional metaverse is anticipated to the be the next step in this evolution. *Business at OECD , Proceedings of Roundtable I*, Paris, May 9, 2023, Privacy in the Metaverse and Immersive Technologies Project.

[3]*Proceedings of the Kick-off Roundtable*, December 15, 2023, Privacy in the Metaverse and Immersive Technologies Project.

[4]Ball, Matthew, *The Metaverse and How It Will Revolutionize Everything* (New York Liveright Publishing, 2022), p. 8.

[5]*Proceedings of the Roundtable I*, op. cit., n. 2; Baker, K. "Designing an Inclusive Metaverse," *Harvard Business Review*, September 22, 2023, https://hbr.org/2022/09/designing-an-inclusive-metaverse.

[6]Digital Regulation Cooperation Form (DCRF) has reported experts' predictions that by 2030 migration to the metaverse will render televisions and smartphones obsolete, while others doubt whether immersive technologies will be adopted broadly. Digital Regulation Cooperation Forum, "Immersive Technologies Foresight Paper," p. 10, December 2023, https://www.drcf.org.uk/__data/assets/pdf_file/0027/273195/DRCF-Immersive-Technologies-Foresight-Paper.pdf.

[7]McKinsey, "Meet the metaverse: Creating real value in a virtual world," June 15, 2022, https://www.mckinsey.com/about-us/new-at-mckinsey-blog/meet-the-metaverse-creating-real-value-in-a-virtual-world.

[8]Ibid.

[9]Throughout this paper the term "privacy" is used to refer to both privacy and data protection.

[10]The metaverse is also likely to raise broader issues companies will need to address and be accountable for, notably regarding data ethics and responsible innovation. The DRCF report highlights regulatory issues related to the collection of biometric data and questions of data privacy and security as factors that will shape adoption. Digital Regulation Cooperation Forum, op. cit. at n. 6.

[11]*Business at OECD*, *Proceedings of Roundtable III*, Kyoto, October 9, 2023, Privacy in the Metaverse and Immersive Technologies Project.

[12]*Proceedings of the Kick-off Roundtable*, op. cit. at n. 3.

[13]The OECD's AI principles serve as one example of a technology-neutral, risk-based approach to governance designed to allow flexibility as AI is developed and deployed, OECD, *Recommendations of the Council on Artificial Intelligence*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.

[14]Organization for Economic Cooperation and Development, *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, 1980, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188.

[15]Organization for Economic Cooperation and Development, *Recommendations of the Council on Artificial Intelligence*, May 21, 2019, amended November 7, 2023, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449; "Emerging privacy-enhancing technologies: Current regulatory and policy approaches," March 8, 2023, https://www.oecd.org/publications/emerging-privacy-enhancing-technologies-bf121be4-en.htm; *Recommendation of the Council on Children in the Digital Environment*, February 16, 2012, amended May 31, 2021; https://legalinstruments.oecd.org/public/doc/272/272.en.pdf.

[16]*Proceedings of Kick-off Roundtable*, op, cit. n. 3. It was also noted at this meeting that the metaverse itself may serve as a platform that supports solutions to address these issues.

[17]*Proceedings of Roundtable III*, op. cit., n. 11; World Economic Forum, "Metaverse Privacy and Safety," pp. 41-43, https://www3.weforum.org/docs/WEF_Metaverse_Privacy_and_Safety_2023.pdf.

[18]Asia Pacific Economic Cooperation, "APEC Privacy Framework," December 2005, https://www.apec.org/publications/2005/12/apec-privacy-framework.

[19]Ball, M., op. cit., n. 4, pp. 59. In his book, Ball presents a foundational definition and description of the metaverse.

[20]*Proceedings of Roundtable I* op. cit. n. 2.

[21]The connectivity and interoperability needed to support the metaverse is said to require a new, more decentralized architecture for the Internet, often referred to as Web 3.0. Paul, L. G., "What is Web 3.0: Definition, Guide and History," *TechTarget*, https://www.techtarget.com/searchcio/tip/10-core-features-of-Web-30-technology#:~:text=Published%3A%2008%20Feb%202023,go%20away%20any%20time%20soon.

[22]PWC, "Demystifying the Metaverse: What Business Leaders Need to Know and Do," https://www.pwc.com/us/en/tech-effect/emerging-tech/demystifying-the-metaverse.html.

[23]"Beyond Reality: The Pivotal Role of AI in the Metaverse," July 28, 2023, https://www.researchgate.net/publication/373116373_Beyond_Reality_The_Pivotal_Role_of_Generative_AI_in_the_Metaverse.

[24]World Economic Forum, "Metaverse Privacy and Safety, op. cit., n. 17, p. 16.

[25]National Institute of Standards and Technology, United States Department of Commerce, "Biometrics at NIST – Identity and Access Management," https://www.nist.gov/identity-access-management/biometrics-nist

[26]https://businesslawtoday.org/2022/08/what-is-inferred-data-why-is-it-important/#:~:text=In%20summary%2C%20inferred%20data%20is,or%20indirectly%20from%20a%20person.

[27]Roundtree, L., "Inferred vs. Observed Data: Do You Really Know the Difference?" *Exchange Wire*, March 2016, https://www.exchangewire.com/blog/2016/03/22/inferred-vs-observed-data-do-you-really-know-the-difference/.

[28]https://www.fgdc.gov/metadata/iso-standards.

[29]"What is Geospatial Data?" IBM, Think, https://www.ibm.com/topics/geospatial-data.

[30]Tunggal, A., "What is Psychographic Data?" *Upguard*, https://www.upguard.com/blog/psychographic-data#:~:text=Psychographic%20data%20is%20information%20about,triggers%20motivate%20them%20to%20action.

[31]Cureton, D., "The Role of the Avatar in the Metaverse," *XR Today*, April 4, 2023, https://www.xrtoday.com/virtual-reality/the-role-of-the-avatar-in-the-metaverse/

[32]However, in some situations, such as gaming, other kinds of avatars that are not as lifelike, may be appropriate. "The Power of Multiple Avatars: Why One is Not Enough," *Union Avatars*, March 2023 https://unionavatars.com/the-power-of-multiple-avatars-why-one-is-not-enough/.

[33]The Internet of Things will serve as one important source of this data. Ball, M. op. cit., n. 4, pp. 157-158.

[34]McKinsey, "Digital Twins: From One Twin to the Enterprise Metaverse, October 2022, https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/digital-twins-from-one-twin-to-the-enterprise-metaverse.

[35]McKinsey, "Digital Twins: The Foundation of the Enterprise Metaverse," October 2022, https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/digital-twins-the-foundation-of-the-enterprise-metaverse. According to McKinsey, "the 'enterprise metaverse' will be powered by dozens of interconnected digital twins that replicate everything from physical assets (like products and office buildings) to people (such as customers and employees) to core business processes and often interact with the physical environment without human intervention."

[36]Reed Smith, "Guide to the Metaverse, 2nd Edition," August 2022, p. 33, https://www.reedsmith.com/en/perspectives/metaverse.

[37]*Proceedings of Roundtable I* op. cit., n. 2.

[38]World Economic Forum, "Metaverse Privacy and Safety," op. cit., n. 17, p. 45.

[39]V. Chamola, G. Bansal, et al., "Beyond Reality: the Pivotal Role of Generative AI in the Metaverse," July 28, 2023, p. 1, https://www.researchgate.net/publication/373116373_Beyond_Reality_The_Pivotal_Role_of_Generative_AI_in_the_Metaverse.

[40]Digital Regulation Cooperation Forum, *Immersive Technologies Foresight Paper*, December 2023, p. 6, https://www.drcf.org.uk/__data/assets/pdf_file/0027/273195/DRCF-Immersive-Technologies-Foresight-Paper.pdf.

[41]Ibid.

[42]Callum Moates, "The Role of AI in Shaping the Metaverse," *Landvault*, October 6, 2023, https://landvault.io/blog/role-of-ai-metaverse#.

[43]Okoro, I., "Sensors and Tracking: The Backbone of Immersive XR Experiences," *Medium*, Sept. 21, 2023, https://medium.com/imisi3d/sensors-and-tracking-the-backbone-of-immersive-xr-experiences-fe7452b33631.

[44]Ibid.

[45]Ibid.

[46]*Proceedings of Roundtable I.* op. cit. n. 2.

[47]*Proceedings of Roundtable III.* op. cit., n. 11.

[48]McKinsey, "Value Creation in the Metaverse," June 2022, p. 5. https://www.mckinsey.com/~/media/mckinsey/business%20functions/marketing%20and%20sales/our%20insights/value%20creation%20in%20the%20metaverse/Value-creation-in-the-metaverse.pdf.

[49]Leading business sectors worldwide that have already invested in the metaverse as of March 2022," Statista, 2023, https://www.statista.com/statistics/1302091/global-business-sectors-investing-in-the-metaverse/.

[50]McKinsey, "Value Creation in the Metaverse," op. cit., n. 41, p. 6.

[51]Christiensen, L., and Robinson, A., "The Potential Global Economic Impact of the Metaverse," The Analysis Group, 2022, p. 12, https://www.analysisgroup.com/globalassets/insights/publishing/2022-the-potential-global-economic-impact-of-the-metaverse.pdf.

[52]MIT Technology Review Insights, "The emergent industrial metaverse," MIT Technology Review, March 29, 2023, https://www.technologyreview.com/2023/03/29/1070355/the-emergent-industrial-metaverse/.

[53]*Proceedings of Roundtable III*, op. cit., n. 11.

[54]Ibid.

[55]Ibid.

[56]Ibid. See also, Slessor, J., "Protecting and Serving in the Metaverse Continuum," *Public Safety Vision* 2022, Accenture, October 13, 2022, https://www.accenture.com/us-en/blogs/voices-public-service/public-safety-tech-vision.

[57]Thorpe, V., "Policing in the metaverse: the opportunities and challenges of immersive technology," *techUK*, March 2022. https://www.techuk.org/resource/policing-in-the-metaverse-the-opportunities-and-challenges-of-immersive-technology.html.

[58]Baker, K. "Designing an Inclusive Metaverse," *Harvard Business Review*, https://hbr.org/2022/09/designing-an-inclusive-metaverse

[59]"Disaster Metaverse with Machine Vision Aerial Drones," *MIT Solve*, Massachusetts Institute of Technology, 2024, https://solve.mit.edu/challenges/climate-adaptation-challenge/solutions/76556#.

[60]"Digital Twins: The Foundation of the Enterprise Metaverse," McKinsey, October 2022, https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/digital-twins-the-foundation-of-the-enterprise-metaverse.

[61]Howland, A., *Fast Company*, "An Interoperable Future for the Enterprise Metaverse" November 3, 2023, https://www.fastcompany.com/90974377/an-interoperable-future-for-the-enterprise-metaverse#:~:text=The%20enterprise%20metaverse%20increases%20efficiencies,teams%20to%20more%20effectively%20collaborate.

[62]Wang, G., Badal, A., *Nature Machine Intelligence*, "Development of metaverse for intelligent healthcare," November 15, 2022, https://www.nature.com/articles/s42256-022-00549-6.

[63]*Proceedings of Roundtable I*, op. cit., n. 2.

[64]One example of this development is Case Western Reserve University's use of the metaverse to facilitate collaboration among geographically distant medical professionals to map a complex surgery. This kind of consultation once required several days of conference calls; in the metaverse, the surgeons are able to complete their planning in approximately an hour. *NBC Nightly News*, August 7, 2022, "Inside the Metaverse: 3D detailed anatomical renderings revolutionizing health care."https://www.nbcnews.com/nightly-news-netcast/video/nightly-news-full-broadcast-january-4th-201384517727?cid=sm_npd_nn_tw_nn.

[65]Access Partnership, "Exploring the Benefits of a Future Metaverse," p. 8, January 2023, https://accesspartnership.com/wp-content/uploads/2023/01/Exploring-the-benefits-of-a-future-metaverse.pdf.

[66]Ibid., p. 9.

[67]*NBC Nightly News* op. cit., n. 57.

[68]Kenya's anticipated Kenya-KAIST virtual campus aims to create a metaverse where students from across the globe can participate in an immersive learning experience and engage in host of campus activities. "The Educational Metaverse is Coming," *KAIST News*, December 2021, https://www.timeshighereducation.com/campus/educational-metaverse-coming

[69]Access Partnership, op.cit., n. 58 at p. 15.

[70]Garaj, G., Dudley, J., Kristensson P. "Five Ways the Metaverse Could Be Revolutionary for People with Disabilities," Brunel University London, September 1, 2022, https://www.brunel.ac.uk/news-and-events/news/articles/Five-ways-the-metaverse-could-be-revolutionary-for-people-with-disabilities.

[71]Pimentel, D., Fauville, Go., et al. "An Introduction to Learning in the Metaverse," Meridian Treehouse, April 2022, pp. 5-6.

[72]Kishore, S., Navarro, X., Dominguez, E., De La Peña, N., & Slater, M. (2018). Beaming into the news: a system for and case study of tele-immersive journalism. *IEEE Computer Graphics and Applications*, 38(2), 89-101, March/April 2018, https://www.researchgate.net/publication/303532865_Beaming_into_the_News_A_System_for_and_Case_Study_of_Tele-Immersive_Journalism.

[73]"A Whole New World: Education Meets the Metaverse," Center for Universal Education at Brookings, February 2022, pp. 1-2, 8, https://www.brookings.edu/wp-content/uploads/2022/02/A-whole-new-world_Education-meets-the-metaverse-FINAL-021422.pdf.

[74]Pimentel, D., Fauville, G., et al. op. cit., n. 64, p. 6. https://static1.squarespace.com/static/5ebf125cd7828b7fb425e1d7/t/624dbe595a03ab107733782e/1649268749694/IntroductionLearningMetaverse-April2022-MeridianTreehouse.pdf.

[75]Meehan, M., "The Metaverse: A New Frontier for Business, Investment," *Forbes*, https://www.forbes.com/sites/forbesfinancecouncil/2022/03/08/the-metaverse-a-new-frontier-for-business-investment/?sh=2d452aae2be9.

[76]Bechtel, M., Launder, N., "Thinking about investing in the metaverse? Let history be your guide," Deloitte Insights, https://www2.deloitte.com/us/en/insights/topics/digital-transformation/metaverse-in-gusiness.html.

[77]Ibid.

[78]"Top 8 Metaverse Business Opportunities to Explore in 2023 and Beyond," PixelPlex, July 30, 2023, https://pixelplex.io/blog/best-metaverse-business-opportunities/#.

[79]*Proceedings of Roundtable I,* op. cit., n. 2, Researchers estimate that to convincingly render a scene, VR headsets track a dozen different types of movements at a rate of 90 times per second; XR applications produce one terabyte of data per hour, which is the equivalent of 200,000 5-minute songs; 310,00 pictures; or 500 hours of movies. Jerome, J. and Greenberg, J. "Augmented Reality + Virtual Reality: Privacy & Autonomy Considerations in Emerging, Immersive Digital Worlds," Future of Privacy Forum, 2021, https://fpf.org/wp-content/uploads/2021/04/FPF-ARVR-Report-4.16.21-Digital.pdf.

[80]Future of Privacy Forum, Ibid.

[81]The need for workable guidance that does not impede innovation would suggest an approach governance that takes into account the varying levels of data sensitivity. *Proceedings of Roundtable I*, op. cit., n. 2.

[82]"[T]he most basic data-stream needed to interact with a virtual world, *simple motion data* may be all that's required to uniquely identify a user within a large population." "Privacy in the Metaverse Might Be Impossible: New Research Study," *Medium*, March 2023, https://medium.com/predict/privacy-in-the-metaverse-might-be-impossible-new-research-study-64935481c6de.

[83]Moates, C., "How Data and Analytics Drive Positive ROI in the Metaverse," Landvault, October 18, 2023, https://landvault.io/blog/data-and-analytics-metaverse

[84]*Proceedings of Roundtable III*, op. cit., n. 11. The GDPR distinguishes data "controllers" and data "processors." It defines data controllers as "the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data."; a data processor is "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller."

[85]*Proceedings of Kick-off Roundtable*, op. cit. n. 3.

[86]Elks, S. "AI bots to user data: Is there space for rights in the metaverse?" Reuters, November 12, 2021, https://www.reuters.com/legal/transactional/ai-bots-user-data-is-there-space-rights-metaverse-2021-11-12/.

[87]The Guidelines articulate the principles of 1.) Collection Limitation; 2.) Data Quality; 3.) Purpose Specification; 4.) Use Limitation; 5.) Security Safeguards; 6.) Openness; 7.) Individual Participation; 8.) Accountability. The discussion here is intended to illustrate the policy challenges the metaverse raises with respect to the principles; it is not an exhaustive review.

[88]According to Data Guidance, "It is reported that, within 20 minutes, in a virtual reality, 2 million unique recordings of body language (such as eye movements, face expressions, and skin temperature) are processed.

The collection of such large amounts of personal data within a short period raises issues regarding the transparency of the personal data that is being processed, with the consequence that the end-user is not informed properly, which complicates obtaining informed, explicit, and specific consent." It further states, "In addition, if different purposes for processing are merged and the individual is not able to consent for each purpose separately, but only for a bundle of purposes, there is a lack of freedom and thus the consent is presumed not to be freely given. Asking for separate consent is expected to be difficult due to the large amounts of data and affects its user-friendliness." https://www.dataguidance.com/opinion/eu-privacy-and-security-concerns-metaverse.

[89]The extent of the challenges AI presents to transparency are reflected in the three-step guidance issued by the UK ICO, which companies are advised to adapt based on their level of expertise and the nature of the organization.https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/explaining-decisions-made-with-artificial-intelligence/.

[90]*Proceedings of Kick-off Roundtable*, op. cit., n. 3. The GDPR, for example, establishes the age of consent at 13; the Thai data protection law sets it at 20.

[91]UK Information Commissioner's Office, *Age-Appropriate Design:* A Code of Practice for Online Services, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/.

[92]Data Protection Commission of Ireland, *Fundamentals for a Child-Centered Approach to Data Processing*, https://www.dataprotection.ie/en/dpc-guidance/fundamentals-child-oriented-approach-data-processing.

[93]CNIL, *Digital Rights of Children*, https://www.cnil.fr/en/digital-rights-children.

[94]In addition to these measures, in May 2022, the European Commission released a new *European Strategy for a Better Internet for Kids*, designed to support implementation of inter alia, the EU's GDPR. The General Data Protection Law recently enacted in Brazil includes specific provisions regarding for the governance of children's data. Recently proposed changes to federal privacy law in Canada address children's privacy more directly. While Japan's Act on the Protection of Personal Information (APPI) does not include provisions that specifically regulate the processing of children's data, General Guidelines on the APPI issued by Japan's Personal Information Protection Commission establishes guidance regarding obtaining consent from minors.

[95]IEEE Standard for an Age Appropriate Digital Services Framework Based on the 5Rights Principles for Children, November 30, 2021, https://standards.ieee.org/ieee/2089/7633/; Information security, cybersecurity and privacy protection— Age assurance systems —Framework [DRAFT] https://www.iso27001security.com/html/27566.html.

[96]United Nations Human Rights Office of the High Commissioner, General comment No. 25 (2021) on children's rights in relation to the digital environment, CRC/C/GC/25, March 2, 2021. https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation

[97]Organization for Economic Cooperation and Development, *Recommendation on Children in the Digital Environment*, February 15, 2012, amended May 30, 2021, https://www.oecd.org/digital/children-digital-environment/#:~:text=OECD%20Recommendation%20on%20Children%20in%20the%20Digital%20Environment&text=The%20Recommendation%20sets%20out%20principles,importance%20of%20international%20co%2Doperation.

[98]Organization for Economic Cooperation and Development, *Recommendations of the Council on Artificial Intelligence*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449; Future of Privacy Forum, (in collaboration with ADP, LinkedIn, Indeed and Workday), *Best Practices for AI and Workplace Assessment Technologies*; https://fpf.org/wp-content/uploads/2023/09/FPF-Best-Practices-for-AI-and-HR-Final.pdf; Center for Democracy and Technology, *AI and Machine Learning*, https://cdt.org/ai-machine-learning/. The CDT document recognizes the evolutionary nature of AI and proposes concepts of fairness, explain-ability, auditability, and accuracy as the foundation for guidance principles.

[99]"Companies Need to Prove They Can Be Trusted with Technology," *Harvard Business Review*, July 21, 2023, https://hbr.org/2023/07/companies-need-to-prove-they-can-be-trusted-with-technology.

[100]*Business at OECD*, *Proceedings of Roundtable II*, Washington, June 27, 2023, Privacy in the Metaverse and Immersive Technologies Project.

[101]OECD Privacy Guidelines, op. cit., n. 14, and n. 80.

[102]*Proceedings of Roundtable II*, op. cit., n. 93.

[103]*Proceedings of Roundtable II*, op. cit. n. 93.

[104]The Australian Privacy Principles, which form the foundation of the Australia Privacy Act of 1988 https://www.apec.org/publications/2005/12/apec-privacy-framework, and Japan's Act on the Protection of Personal Information (Act No. 57 of 2003), https://www.japaneselawtranslation.go.jp/en/laws/view/4241/en are examples of data protection laws that reflect the Guideline's principles.

[105]The EU-U.S. Data Privacy Framework, and the related UK Extension to the EU-U.S. DPF, and Swiss-U.S. DPF were respectively developed by the U.S. Department of Commerce and the European Commission, UK Government, and Swiss Federal Administration to provide U.S. organizations with reliable mechanisms for personal data transfers to the United States from the European Union, United Kingdom, and Switzerland while ensuring data protection that is consistent with EU, UK, and Swiss law. https://www.dataprivacyframework.gov/s/.

[106]"APEC Privacy Framework," op. cit., n. 18, In addition to the eight principles articulated in the OECD Privacy Guidelines, the APEC Privacy Framework also includes the principle of "Prevention of Harm."

[107]The APEC Cross-border Privacy Rules (CBPR) system is a government-backed data privacy certification that companies can join to demonstrate compliance with internationally recognized data privacy protections. The CBPR system implements the APEC Privacy Framework, which was endorsed by APEC Leaders in 2005 and updated in 2015. The CBPR system is designed to benefit consumers and business by ensuring that regulatory differences do not impede businesses' ability to deliver products and services. https://www.apec.org/about-us/about-apec/fact-sheets/what-is-the-cross-border-privacy-rules-system.

[108]*Proceedings of Roundtable II*, op. cit., n. 93; Organization for Economic Cooperation and Development, *The OECD Privacy Framework*, 2013, pp. 3-4, https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

[109]Ibid. at pp. 12, 16, and 30.

[110]Ibid. at p. 16.

[111]*Proceedings of Roundtable II*, op. cit., n. 93.

[112]*Proceedings of Roundtable II*, op. cit., n. 93, Organization for Economic Cooperation and Development, *Report on the Implementation of the Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, p. 6, 2021, https://one.oecd.org/document/C(2021)42/en/pdf.

[113]bid. at p. 60.

[114]Ibid. at p. 7, 49-51.

[115]Organization for Economic Cooperation and Development, *Recommendation of the Council concerning Guidelines for Cryptography Policy* [C(97)62, 2024, https://legalinstruments.oecd.org/public/doc/115/115.en.pdf; *Recommendation of the Council on Electronic Authentication* [C(2007)68], 2024, https://legalinstruments.oecd.org/public/doc/120/120.en.pdf; *Recommendation of the Council on the Protection of Children Online* [C(2011)155], 2012, https://www.google.com/search?client=safari&rls=en&q=Recommendation+of+the+Council+on+the+Protection+of+Children+Online+%5BC(2011)155%5D&ie=UTF-8&oe=UTF-8.

[116]*Proceedings of Roundtable III*, op. cit., n. 11.

[117]Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, https://gdpr-info.eu.

[118]The GDPR defines a data controller as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law." It defines a data processor as a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.

[119]Privacy by design is discussed at more length in section VIII.

[120]*Proceedings of Roundtable III*, op. cit., n. 11.

[121]Organization for Economic Cooperation and Development, forthcoming.

[122]Ibid

[123]"Implementing OECD AI Principles: Challenges and Best Practices," *Business at OECD*, 2023, https://www.businessatoecd.org/blog/implementing-oecd-ai-principles-challenges-and-best-practices

[124]Seven principles, articulated by former Ontario Information and Privacy Commissioner Ann Cavoukian, guide privacy by design. Cavoukian, A. "Privacy by Design: The 7 Foundational Principles Implementation and Mapping of Fair Information Practices, https://www.ietf.org/slides/slides-privacyws-privacy-by-design-the-seven-foundational-principles-00.pdf

[125]Ibid.

[126]Implementing privacy by design into an existing system requires a more burdensome, less effective process involving deconstruction and analysis of an existing system and retrofitting solutions. *Proceedings of Roundtable I*, op. cit., n. 2.

[127]Privacy-enhancing technologies can serve as useful tools for managing privacy risks. For example, advances in encryption and differential privacy can allow for privacy-preserving data analysis and sharing, and the use of synthetic data sets can alleviate concerns about data sharing or secondary data use.

[128]Tsvalis, T., "The Metaverse Dilemma: Privacy Concerns in Virtual Worlds," *Forbes*, October 23, 2023, https://www.forbes.com/sites/forbestechcouncil/2023/10/23/the-metaverse-dilemma-privacy-concerns-in-virtual-worlds/

[129]Stefanic, D., "Security and Privacy in Metaverse Events," *Hyperspace: Metaverse for Business*, December 5, 2023, https://hyperspace.mv/security-and-privacy-in-metaverse-events/.

[130]"Privacy-Enhancing and Privacy Preserving Technologies: Understanding the Role of PETs and PPTs in the Digital Age, Centre for Information Policy Leadership," December 2023, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-understanding-pets-and-ppts-dec2023.pdf.

[131]McMahan, B. and Ramage, D. "Federated Learning: Collaborative Machine Learning without Centralized Training Data," *Google Research*, April 6, 2017, https://blog.research.google/2017/04/federated-learning-collaborative.html?m=1.

[132]OECD, Recommendation of the Council on Enhancing Access to and Sharing of Data. 2021. https://www.oecd.org/mcm/Recommendation-of-the-Council-on-Enhancing-Access-to-and-Sharing-of-Data_EN.pdf

[133]*Proceedings of Roundtable I*, op. cit., n. 2.

[134]Emmatty, L., "Securing Digital Identity in the Metaverse: A Global Imperative," https://blog.ccgrouppr.com/blog/securing-digital-identity-in-the-metaverse-a-global-imperative

The UK government is developing a framework of rules which show what 'good' digital identities look like. The 'trust framework' articulates rules organisations should follow, including the principles, policies, procedures, and standards governing the use of digital identity. The framework sets out areas such as: how organisations should handle and protect people's data; what security and encryption standards should be followed; how user accounts should be managed; and how to protect against fraud and misuse. Once finalized, the framework is expected to be codified into law. "UK digital identity and attributes trust framework alpha v2 (0.2), https://www.gov.uk/government/publications/uk-digital-identity-attributes-trust-framework-updated-version.

[135]Because data protection requirements may vary across jurisdictions, organizations are still faced with reconciling various and sometimes competing obligations in law. Regulator guidance about the role of PETs in compliance could help organizations make better-informed implementation choices. CIPL paper cite.

[136]CIPL and Cisco, "Business Benefits of Investing in Data Privacy Management Programs," January 2023, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cisco-cipl_report_on_business_benefits_of_investing_in_data_privacy_management_programs__10_jan_2023_.pdf. 19 3. Adoption and Deployment of PETs within Organizations.

[137]Ibid.

[138]*Proceedings of Roundtable II*, op. cit., fn. 93.

[139]Ibid. Privacy by design can be implemented in coordination with other requirements that protections be incorporated into a device or offering's architecture, including user safety and protections for children.

[140]Ibid.

[141]Ibid.

[142]XR Association, Statement of XR Association's "Basic Beliefs" on privacy, https://xra.org/public-policy/privacy/

[143]XRSI, "The XRSI Privacy and Safety Framework," https://xrsi.org/publication/the-xrsi-privacy-framework.

[144]The Metaverse Standards Program, https://metaverse-standards.org.

[145]IEEE Standards Association, The IEEE Global Initiative on Ethics of Extended Reality, https://standards.ieee.org/industry-connections/ethics-extended-reality/.

[146]The standards include Extended Reality Augmented Reality, Virtual Reality, Immersive Web and Spatial Web technologies.

[147]IEEE Standards Association, IEEE P7030 Working Group, https://sagroups.ieee.org/7030/#:~:text=Scope%3A%20This%20standard%20establishes%20a,positive%20design%20of%20XR%20systems.

[148]Ibid.

[149]https://fpf.org/about/.://fpf.org/about/.

[150]Jerome, J., Greenberg, J., "Augmented Reality and Virtual Reality: Privacy & Autonomy Considerations in Emerging, Immersive Digital Worlds," Future of Privacy Forum, April 2021, https://fpf.org/wp-content/uploads/2021/04/FPF-ARVR-Report-4.16.21-Digital.pdf.

[151]Ibid. at p. 2.

[152]Privacy-enhancing technologies can serve as useful tools for managing privacy risks. For example, advances in encryption and differential privacy can allow for privacy-preserving data analysis and sharing, and the use of synthetic data sets can alleviate concerns about data sharing or secondary data use.

[153]UNICEF, "Responsible Innovation in Technology for Children: Digital technology, play and child well-being," https://www.unicef-irc.org/ritec.

BUSINESSatOECD

THE USCIB FOUNDATION

Business at OECD (BIAC)
13/15, Chaussée de la Muette
75016 Paris, France
+33 (0)1.42.30.09.60
communications@biac.org
@BusinessatOECD

THE USCIB FOUNDATION, INC.
1212 Avenue of the Americas
New York, NY 10036
+1 212-703-5064
info@uscib.org
@USCIB