In collaboration
with Accenture

Metaverse Identity: Defining the Self in a Blended Reality

INSIGHT REPORT

MARCH 2024

Images: Getty Images, Midjourney

Contents

Disclaimer
This document is published by the World Economic Forum as a contribution to a project, insight area or interaction. The findings, interpretations and conclusions expressed herein are a result of a collaborative process facilitated and endorsed by the World Economic Forum but whose results do not necessarily represent the views of the World Economic Forum, nor the entirety of its Members, Partners or other stakeholders.

Foreword

Daniel Dobrygowski
Head, Governance and Trust, Centre for the Fourth Industrial Revolution Digital Technologies, World Economic Forum

Dave Treat
Senior Managing Director, Innovation, Incubation Group Lead, Accenture

The metaverse aims to be the future of the internet – a spatial, social internet experience that uses existing and emerging technologies to seamlessly blend physical and digital worlds. With recent developments in generative artificial intelligence (AI), metaverse creation and growth may expand. While media announcements about AI and the metaverse may compete for media attention, they are, in fact, partners in this digital evolution.

The metaverse will act as a conduit to blend the digital world with the physical world and transform how people interact with information, others and their surroundings. One of the central elements in this advancement is "identity".

In May 2022, the World Economic Forum launched the Defining and Building the Metaverse Initiative, which orchestrates an integrated approach to the development and governance of the metaverse. The initiative is divided into two workstreams: governance and economic and social value creation. It seeks to build a responsible, equitable, inclusive, diverse and accessible metaverse through discussions with a wide array of stakeholders.

This report is a continuation of the World Economic Forum's Defining and Building the Metaverse Initiative. In collaboration with Accenture, previous outputs from this initiative include:

- Interoperability in the Metaverse
- Privacy and Safety in the Metaverse
- Demystifying the Consumer Metaverse
- Social Implications in the Metaverse
- Exploring the Industrial Metaverse

In this report, the governance workstream underscores the imperative for global collaboration in forming a shared understanding of the metaverse and metaverse identity. It aims to set best practices that encourage innovation and growth while safeguarding privacy and security. Ignoring the evolving expectations of identity in the metaverse could lead to repeating current internet shortcomings.

To build a metaverse that is economically vibrant as well as equitable, accessible and inclusive, attention must be given to human rights, equality and sustainability. The report draws on contributions from a diverse global working group of over 150 experts across academia, international organizations, civil society, government, technology and business sectors.

Executive summary

Identity – encompassing representation, data and identification – will be a critical component of the metaverse.

The metaverse, thought of as the future version of the internet, continues to garner research, development and investment interest around the world. It has immense potential to reshape the way individuals live, work and interact.

As the convergence of extended reality (XR) technologies blur the boundaries between physical and virtual worlds, it becomes imperative to address the topic of "identity" to ensure an inclusive, equitable, accessible, secure and privacy-preserving metaverse. This report highlights the role metaverse identity plays in designing human-first experiences[1] and catalyses stakeholders to navigate the complexities of metaverse identity.

Metaverse identity encompasses:

- **Representation**: including personal, social and role identity, be it through avatars, pseudonyms or other digital expressions
- **Data**: capturing the intricate web of knowledge about individuals generated by metaverse-supporting hardware and software
- **Identification (ID)**: be it through driver's licences, government-issued IDs, passports, birth certificates, attestations, labels, or usernames and passwords.

These layers span human identities and the advent of digital entities – avatars, virtual agents, digital replicas and other assets that contribute to the rich tapestry of metaverse inhabitants.

As people spend more time exploring, playing and socializing in digital experiences, a person's metaverse identity will be central to their day-to-day life as well as to the way they express their personal identity. Education on what it is and how to use it safely will be transformational.

Given the broad socio-technical concept of identity, the implications and insights within this document are pertinent to a broader audience beyond those who focus primarily on the construct of digital ID. A multistakeholder, diverse group must come together to navigate identity challenges and sculpt a metaverse that is secure, beneficial and equitable for all. Therefore, metaverse identity requires ongoing input and collaboration from key stakeholders, including:

- Design teams
- Academia
- Business leaders – in diverse fields ranging from security, marketing and HR to strategy
- Government entities – such as policy-makers and law enforcement
- Civil society and stakeholders from other assorted backgrounds – such as standards associations, etc.

While foundational elements of identity management and the myriad of identity system archetypes[2] (e.g. centralized, federated and decentralized systems) and supporting technologies, such as blockchain, remain relevant, this report goes beyond questions of infrastructure and system management.

This report examines identity as a means of crafting digital belonging and presence. By highlighting identity considerations, responsible data practices and inclusive design principles, this report aims to support stakeholders in conversations about how to navigate metaverse identity responsibly and ethically across data, representation, ID and digital entities.

BOX 1

Responsible innovation is key

With the next evolution of the internet, it will be critical to confidently manage the connection between physical humans, associated digital identities and corresponding data. This is necessary to protect individuals, manage content and safely secure services. Responsible innovation is key to bridging the physical and digital worlds in ways that meets societal, legal and cultural needs community by community.

Introduction

Digital identification is expanded in the metaverse through forms of representation, new data types and digital entities.

Metaverse insight

The metaverse aims to be a spatial, social internet experience[3] that uses existing and emerging technologies to seamlessly blend physical and digital worlds. It will enable shared, persistent realities, transforming how people interact with information, others and their surroundings.[4]

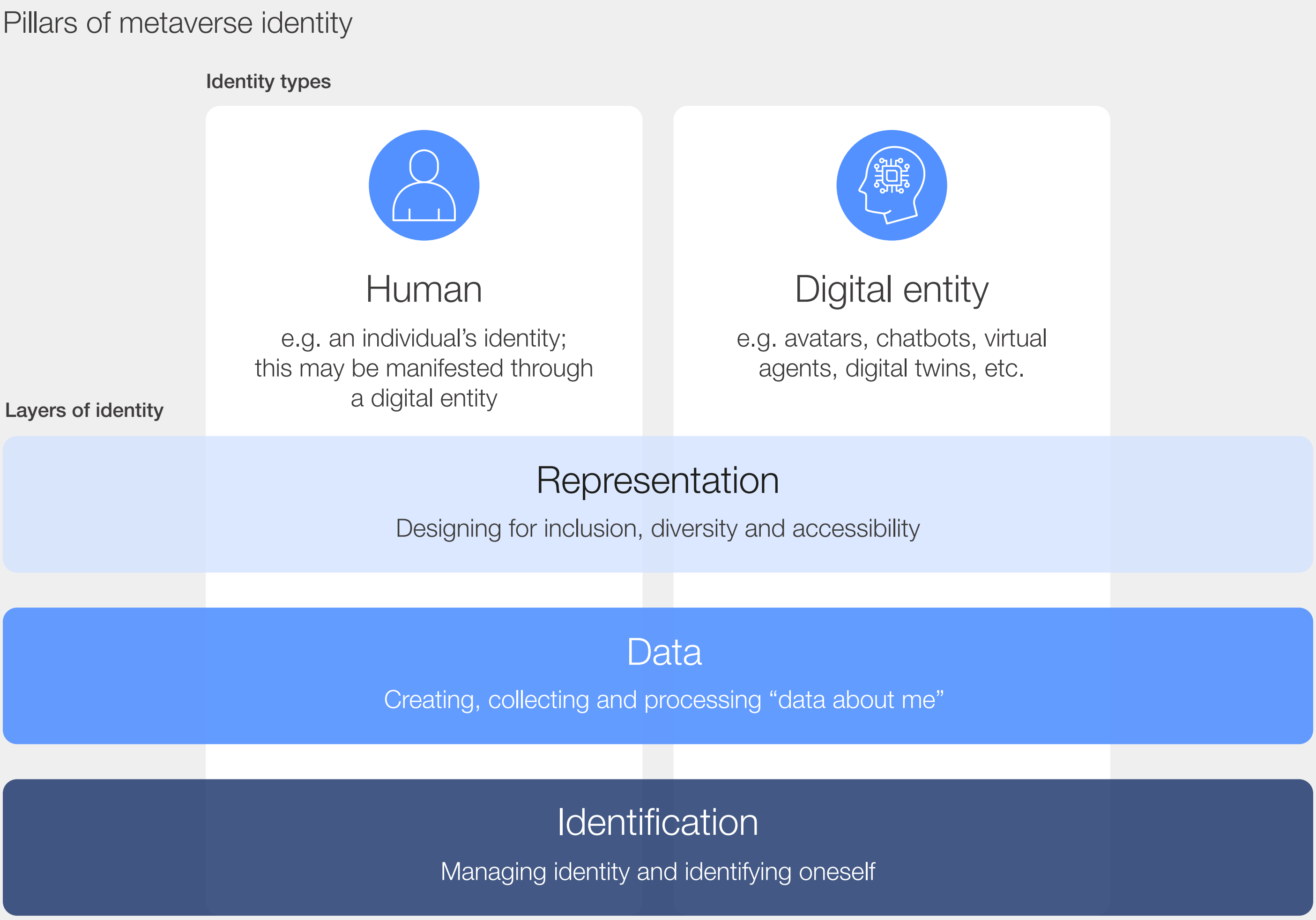
The metaverse has emerged as a vision for the future of the internet – built on the current internet and new spatial experiences.[5,6] This report discusses the importance of metaverse identity and considerations that may set the foundation for an inclusive, privacy-preserving next era of the internet.[7]

Metaverse identity is an extension of identity as it is known today – encompassing forms of representation, data and identification (ID). For example:

- **Representation**: Beyond static profile pictures, users may adopt customizable digital assets – such as avatars, augmented reality (AR) filters and accessories – that reflect various facets of their identity, whether that be cultural attire, distinctive physical features or abstract designs that symbolize personal beliefs or affiliations. These presentations will cover a spectrum of manifestations from real-world appearance to entirely aspirational or creative. These expressions may extend to include words, actions, behaviours and mannerisms. Stakeholders must understand that representation is not limited to immersive experiences, such as virtual reality (VR) and platforms; representation blends physical and digital worlds across traditional 2D screens along with AR and mixed realities (MR).
- **Data**: Data points are capable of describing identity. Paired with artificial intelligence (AI)/machine learning (ML) models that can analyse a person's interactions, movements and preferences further generates identity. Whether these (inferred) data points are capturing a person's current activities, predicting their next action or future preferences, these data-based breadcrumbs provide information into one's identity. These attributes may influence the way the virtual environment responds to an individual, and outsiders perceive an individual or entity.
- **ID**: Similar to today's traditional identification systems – like passports and driver's licences – IDs may evolve to include unique avatar designs, new body-based[8] attestations or unique virtual signatures that validate one's existence and grant access to specific realms or activities.

Metaverse identity extends beyond a tangible human to include digital entities. These encompass a range of entities ranging from simple text-based chatbots to complex, human-like avatars and photo-realistic digital doppelgangers – or digital replicas. Digital entities may represent humans (i.e. via avatars[9,10]), systems (i.e. via chatbots[11,12]), objects (i.e. via digital twins[13,14]) or other abstract concepts[15,16] and are capable of varying degrees of interaction, autonomy and behaviour within digital experiences. Digital entities will be an enabling aspect of metaverse identity, facilitating and augmenting digital interactions.

FIGURE 1 Pillars of metaverse identity


Pillars of metaverse identity
Identity types
Human
e.g. an individual's identity; this may be manifested through a digital entity
Digital entity
e.g. avatars, chatbots, virtual agents, digital twins, etc.
Layers of identity
Representation
Designing for inclusion, diversity and accessibility
Data
Creating, collecting and processing "data about me"
Identification
Managing identity and identifying oneself

Given the well-known global discussion regarding ID, digital ID[17] and system archetypes (centralized, federated and decentralized) of identity infrastructure,[18] this report will:

- Explore the above net-new facets of identity in the future internet, emphasizing the importance of its multi-dimensional nature and its pivotal role in shaping the digital future
- Conceptualize how metaverse identity can bring human-by-design[19] and human-first[20] design requirements into the larger global conversation.

The early development stage of the metaverse presents a unique opportunity to prioritize building a metaverse identity framework that champions inclusivity, accessibility, equity, diversity and sustainability while enabling security and innovation. To achieve this, stakeholders must learn from real-world identity conversations and the challenges of previous internet generations and go forward with purpose. Without these important conversations, stakeholders risk revisiting the mistakes of current online experiences – one that mirrors real-world inequality, privacy concerns and security threats on a vast, nearly infinite digital canvas.

1 Metaverse identity

To navigate metaverse identity, stakeholders must understand its ubiquity and impact on digital interactions, vulnerable populations and personal expression.

Metaverse identity broadens "identity" as it is known today and combines it with the digital underpinnings of the internet. It is a multi-layered construct of an individual or entity, including everything from representation to data and identification.

Metaverse identity connects and anchors a person to the physical and virtual world.

It is the foundation that privacy and security measures protect; it is the building block that enables recognition of the movement of money and objects. As interactions and transactions become more complex and diverse, a robust and adaptable identity framework will become the bedrock upon which digital trust,[21] authenticity and metaverse experiences are built.

1.1 A story about metaverse identity

Imagine a world where the boundaries between the physical and digital realms blur and where this scenario is commonplace.

Morning sun filters through the blinds as future-you rises from bed. Your virtual assistant, sensing you're awake, runs your pre-scripted morning wake-up routine. The companion authenticates you – not just from a password but from your unique voice pattern. Once you are verified, it runs the routine you've requested and reads out both your personal schedule and your work calendar; then, it prioritizes, summarizes and shares messages that were sent to your work email overnight. This morning's read-out puts you in the right mindset to tackle an early meeting in the office.

While prepping for your day, you put on your smart glasses, and they display a message from your mother. You consent to opening the messages, and rather than her text showing, her digital avatar (a close likeness to her real self) appears beside you in AR, relaying the message about a change in dinner plans. Using your smart mirror – and AI filters to make you more presentable so early in the morning – you send a video reply. Meanwhile, your virtual assistant updates your itinerary for the evening and schedules an autonomous vehicle to pick you up after work to drive you to dinner.

Throughout your day at the office, your smart glasses serve a dual purpose. They bring the work-from-home employees into the meeting room to improve accessibility. Additionally, when you speak with colleagues, real-time data overlays provide context – real-time subtitles, recent emails exchanged, upcoming shared events or even mutual contacts – aiding in smoother communication. All this is made possible because your co-workers have given tiered permission access as part of their professional digital identities.

Child insight

Metaverse identity choices made today will affect more than just adults;[22] it will affect how children's information, and the information of other vulnerable groups, is processed.

In this near-future world, metaverse identity may simplify, secure and personalize everyday experiences.[23] It highlights that the movement of a person's identity – across digital and physical spaces – makes identity central to the future of the blended world.

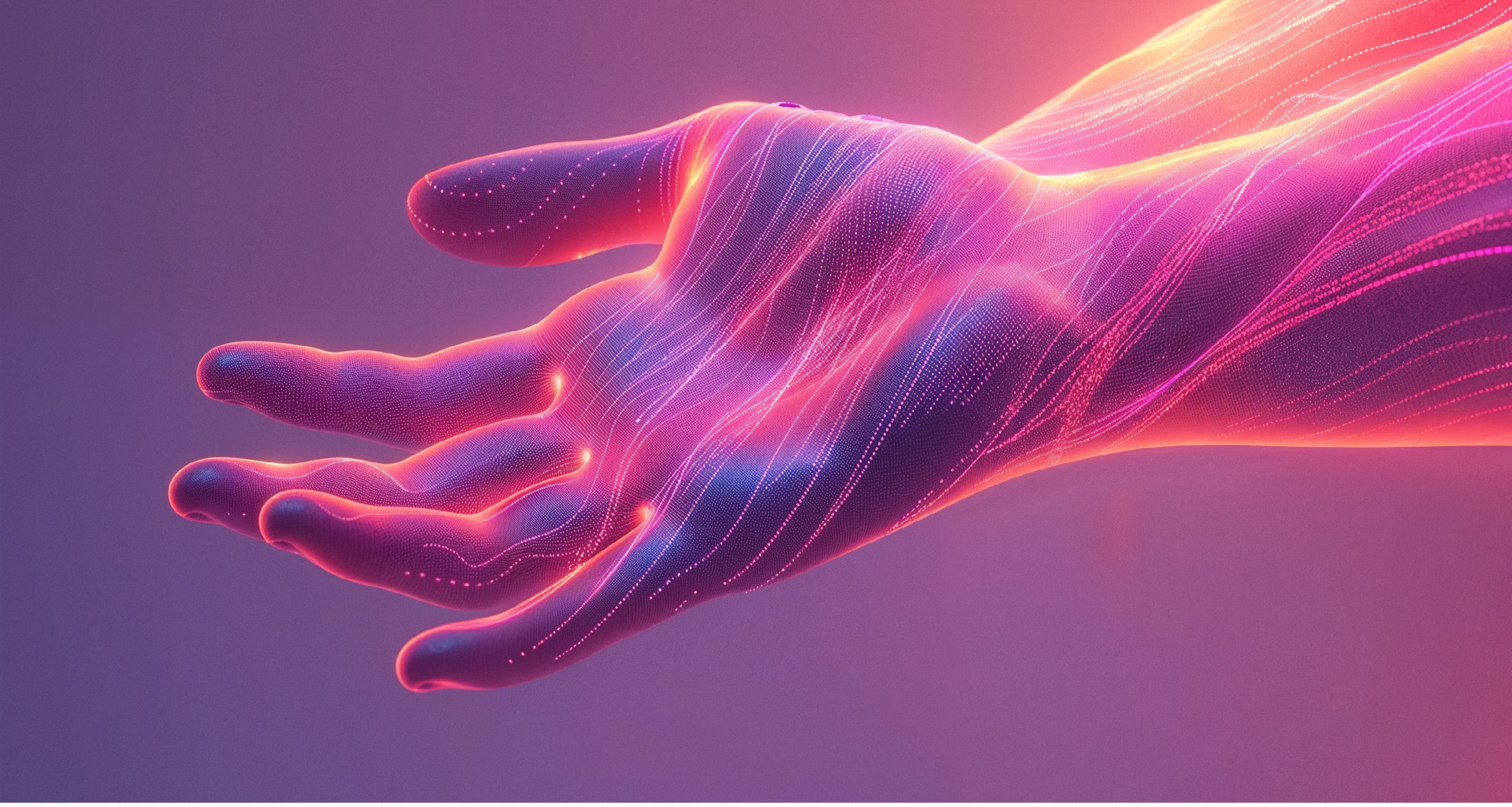
With this frontier comes an essential question: In an environment where the tangible and intangible converge, how can stakeholders best enable the management of data, representation and identification while protecting individuals and encouraging innovation?

1.2 The role of identity

1.2.1 Identity is foundational

The concept of identity is contextual, flexible, complex and fluid. Individually answering the question, "Who am I?" depends on a range of factors, including items such as: when someone asks the question, how one perceives themselves, their membership to certain groups and how others influence one's self-perception.

The answer provided by the individual may differ entirely from the one provided by a third party. For example, whether it's members of one's community or an organization – each will have their own distinct view of how they perceive an individual. This is because the available information, or data, that they have will influence their perception of the individual's identity.



Metaverse insight

> The metaverse offers a realm where identity is not just a concept, but a lived experience, demanding a balance between self-expression and privacy protection.[24]

Identity consists of layered aspects of cultural heritage, ethnicity, age, professional and social roles, hobbies, gender identification, sexual orientation and much more. These elements of identity can be sources of pride and self-expression. Yet, these very same attributes can become vulnerabilities in some contexts. Possession, let alone revealing certain identity facets, may invite bullying, harassment, stalking, discrimination, prosecution, legal action, persecution, grooming[25] or bias. This duality casts a spotlight on the complexities of identity in the real world.

1.2.2 The ID gap

Forms of ID – such as passports and government IDs – formalize an individual's identity; additionally, these can serve as credentials or means of authenticating and verifying individuals across physical and digital spaces.

While the metaverse may open new avenues to formalize ID, stakeholders should remember an often-overlooked challenge termed the "identification gap"[26] – or the number of individuals who do not have a form of ID. This ID gap underscores the importance of ensuring that, as society progresses into the digital era, efforts are made to be inclusive and mindful of those who, by choice or circumstance, remain outside the formal bounds of identification.

1.2.3 Metaverse identity is integral to future internet interactions

The lack of focus on identity may limit the social experiences within digital worlds; it may also have more serious consequences like unintentionally and negatively extending hegemonic[27] or anthropomorphic[28] norms to technology. Improperly designed metaverse identities may:

– Negatively influence social mobility in physical worlds, given the reliance economies have on digital platforms

– Hinder mechanisms to identify privately and securely, credential, authenticate and verify an individual or digital human entity

– Improperly assign human-like qualities and essence to technology, resulting in over-trust and realization of harms ranging from psychological to emotional.

To build an inclusive, economically viable and responsible metaverse, stakeholders should be asking themselves:

1. How will metaverse identity be understood by non-digital natives?
2. How essential will the metaverse be to social and economic engagement?
3. How is identity to be presented, perceived and interoperate across different jurisdictions and metaverse infrastructure models?

1.2.4 The opportunity

Stakeholders must understand and discuss identity beyond the infrastructure foundations and system archetypes that authenticate and manage credentials.

The metaverse presents an opportunity to recognize the individual at the centre of these identity systems through inclusive, accessible and equitable design. The opportunity exists to define, redefine and protect through:

- **Managing representation**: creating inclusive, diverse digital presentation in a new medium – inclusive of avatars or other digital assets – that may mirror real-world aspects of identity or embrace entirely new, imaginative forms
- **Managing data** through privacy-preserving technologies and processes via:
    - Improving consent mechanisms
    - Minimizing and selectively processing collected identity information
    - Increasing transparency regarding data collection, data processing, the purposes for which data will be used and implications of consenting to data collection/processing
    - Maintaining selective anonymity and/or ability to control the disclosure of personal data
- **Managing and facilitating** ID associated experience via:
    - Credentials and wallets
    - Connections between people and digital assets
    - Interactions between people and digital entities

Metaverse insight

> Building a responsible and inclusive metaverse demands a deep understanding of diverse identity expectations and challenges across geographies.[29]

Designing the future of the metaverse requires a nuanced approach to identity[30] that necessitates an inclusive dialogue spanning geographies, ethnicities, gender and sectors to enable inclusivity, diversity, equity and accessibility.

1.3 What is metaverse identity?

This report posits that metaverse identity refers to the manifestation of identity across digital and physical spaces; this encompasses expressions, credentials, data attributes and digital entities.

1.3.1 Who has a metaverse identity?

Metaverse insight

> Everyone has a metaverse identity due to the choices they make both on and offline.
> It's critical that identity holders and other stakeholders alike protect it with sensitivity.

Given that the metaverse is an extension of and an evolution of today's internet, it may be assumed that anyone online today can have a metaverse identity.

Whether it's composed of a photo, a Facebook profile, a Reddit account, a picture, an IP address, a gamer tag, digital wallet address, or something else, everyone online has a collection of digital crumbs that accumulate to form a metaverse identity.

Child insight

Metaverse identities may be linked back to a real-world self; as such, additional considerations around privacy, safety and compliance is needed for the well-being of children and other vulnerable populations.[31]

Metaverse identity extends beyond possessing an avatar and encompasses an individual's behaviours, preferences, movements, actions and decisions made in digital realms – whether they be AR, VR, MR, 2D webpages or something else.

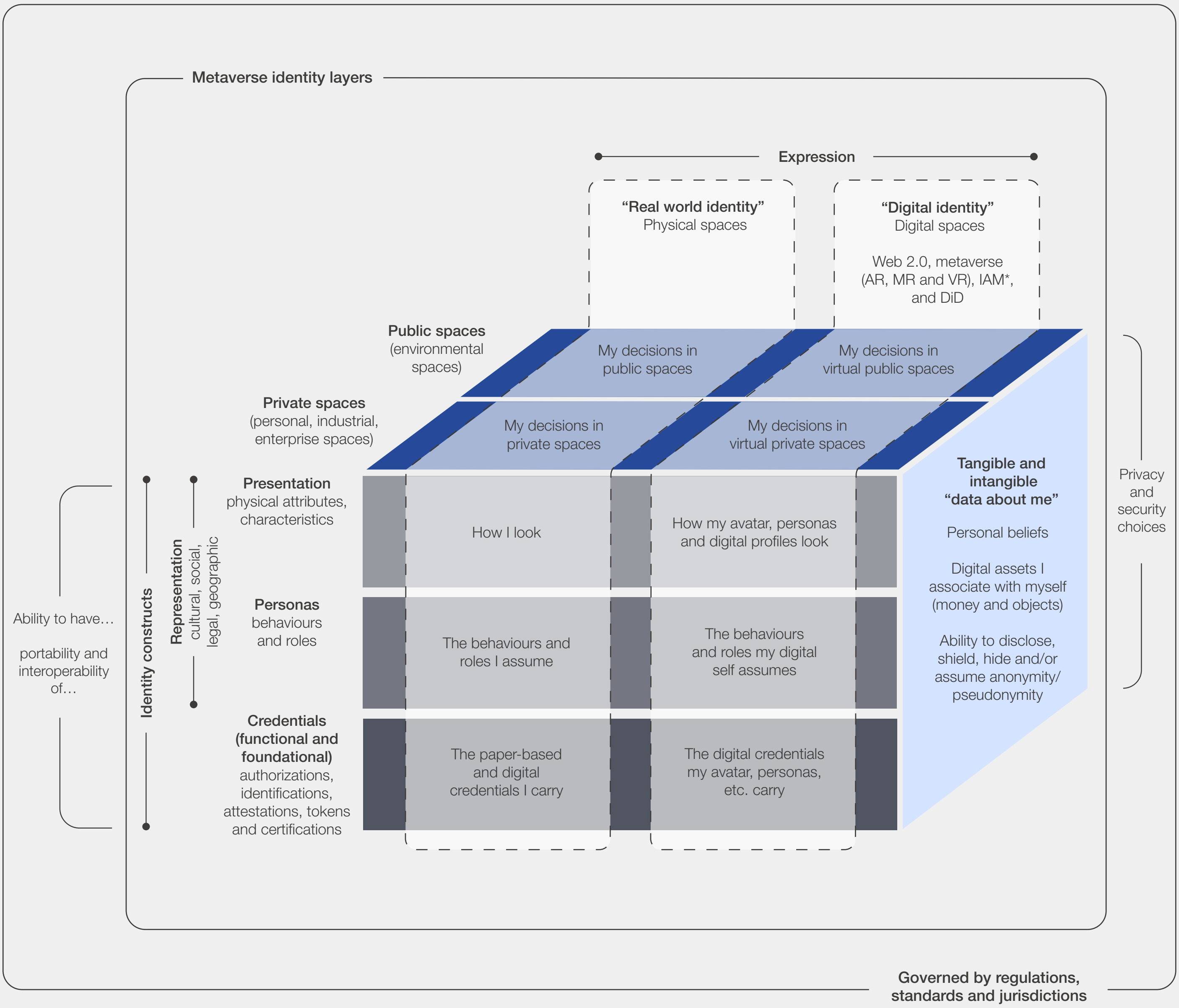
Given this potential traceability between an individual's identity in the digital world and their "real-life" identity in the physical world, stakeholders should consider the tension between privacy, safety, regulation[32] and individual identity choices.

1.3.2 Speaking a common identity language

Metaverse identity is composed of how one presents themselves, the personas they assume and the credentials they possess.

Behind all these layers are the supporting data points that capture the essence of those expressions.

FIGURE 2 **Metaverse identity layers**



Metaverse identity layers
Expression
"Real world identity"
Physical spaces
"Digital identity"
Digital spaces
Web 2.0, metaverse (AR, MR and VR), IAM*, and DiD
Public spaces (environmental spaces)
My decisions in public spaces
My decisions in virtual public spaces
Private spaces (personal, industrial, enterprise spaces)
My decisions in private spaces
My decisions in virtual private spaces
Presentation physical attributes, characteristics
How I look
How my avatar, personas and digital profiles look
Personas behaviours and roles
The behaviours and roles I assume
The behaviours and roles my digital self assumes
Credentials (functional and foundational) authorizations, identifications, attestations, tokens and certifications
The paper-based and digital credentials I carry
The digital credentials my avatar, personas, etc. carry
Tangible and intangible "data about me"
Personal beliefs
Digital assets I associate with myself (money and objects)
Ability to disclose, shield, hide and/or assume anonymity/ pseudonymity
Privacy and security choices
Identity constructs
Representation cultural, social, legal, geographic
Ability to have…
portability and interoperability of…
Governed by regulations, standards and jurisdictions

*Identity and access management
**Decentralized identifiers

1.3.3 Special attention is required

Child insight

As children craft their digital identities, they may inadvertently share sensitive information, making them susceptible to various online risks.[33] Digital intermediaries, agents and guardians may offer a solution.

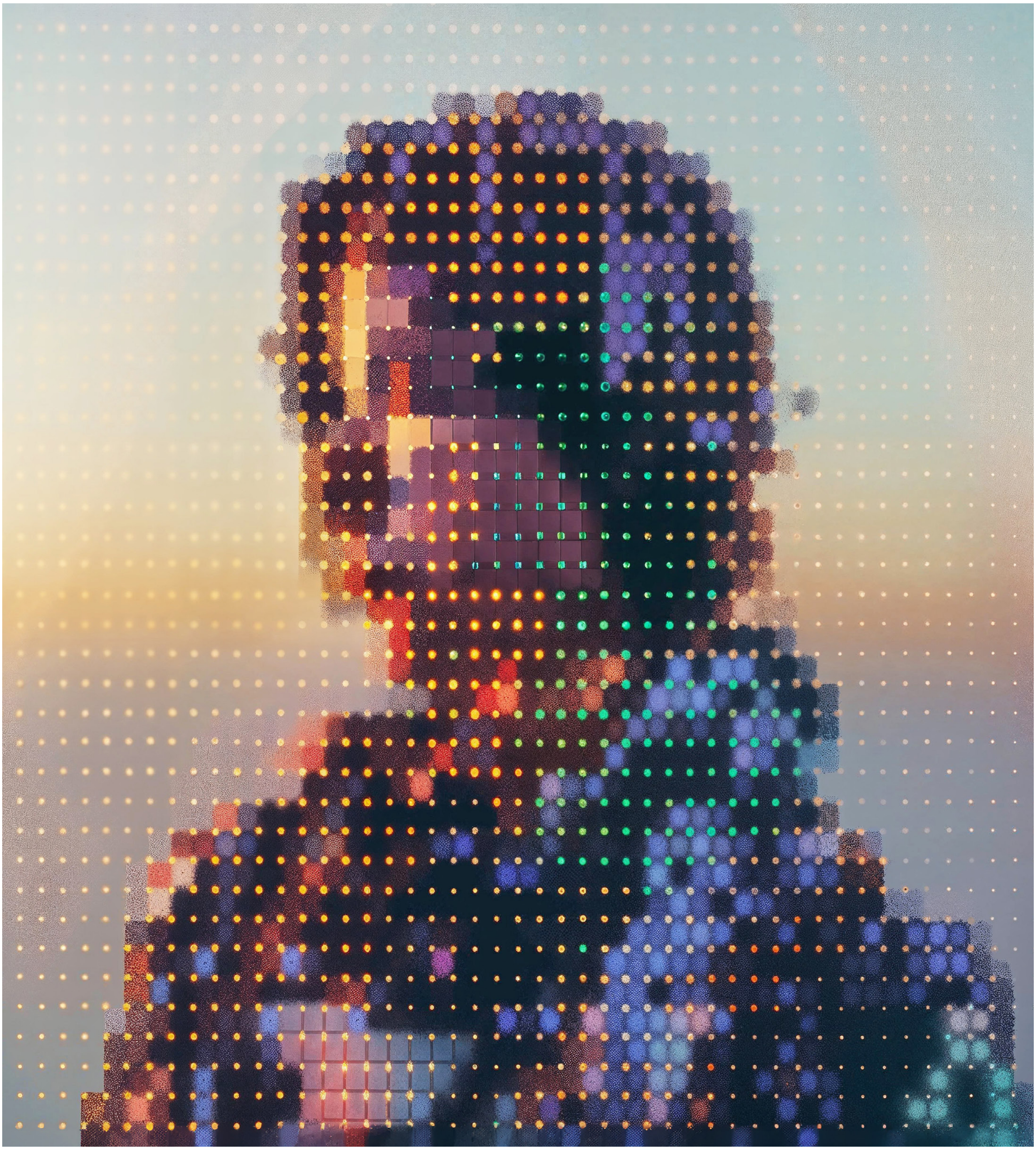
The importance of addressing privacy and safety[34] cannot be understated as individuals, and particularly vulnerable individuals, start onboarding to metaverse experiences.

Vulnerable populations – including children, populations with limited technological proficiencies or individuals with cognitive challenges affecting decision-making abilities – have limited capacity for discernment, which requires heightened considerations for privacy and safety provided by parents, platforms and regulators alike.

Vulnerable populations are more susceptible to online risks. Recognizing this, the introduction of both AI-driven and manually managed virtual guardians[35] – or specialized virtual assistants[36] – might offer a solution, acting as protective buffers. This could help manage and oversee an individual's interactions, ensuring that their metaverse experiences are enriching, privacy-preserving and safe while navigating the intrinsic tension between exploration and protection.

2 Inferring identity from data

New data types will identify users in new, more subtle ways, requiring a new lexicon and responsible data processing.



2.1 Your metaverse identity generates data

Metaverse insight

Identity goes beyond ID, like a passport or driver's licence. Metaverse identity includes data points.[37]

Identity extends into the intricacies of an individual's behaviours, actions and choices.

The way an individual speaks – for example, with unique tonal inflexions or cultural idioms – can offer insights into their background and upbringing. Similarly, a person's distinctive movements, whether it's the fluidity of their dance or the precision of their basketball shots, tell tales of their experiences and passions. Collectively, these attributes can generate insights and inferred data.

Inferred data revolves around deriving insights from information through pattern recognition within data. Inferred data[38] is not new. This sophisticated analytical process, now aided by AI/ML, can examine seemingly unrelated behaviours, actions and choices to draw meaningful conclusions about a person's preferences, background and intentions.

However, the new types of data available with the rise of the metaverse and supporting technologies will fundamentally shift the level of information available regarding "data about me".[39]

2.2 How metaverse identity data is processed matters

Statista expects that by 2025 nearly 181 zettabytes of data will be created, captured, copied and consumed worldwide.[40] That is nearly a 1,075% increase from 2015.[41] Stakeholders must consider and plan for the depth and breadth of this data.

Metaverse insight

Use of AI/ML must adhere to responsible AI practices and principles including those relating to human rights, transparency, human autonomy and non-discrimination.[42]

The implications of data and inferred data in the identity space can present challenges. For example, imagine a virtual world where individuals can customize their experience. A platform or system may track every customization choice and corresponding data point an individual makes over time.

- While this data is collected to enhance the person's experience, it could also be analysed to make inferences as to their real-world identity or preferences and used for targeted advertising or other purposes without their consent.[43,44]
- Given that identity is contextual on circumstance, these data points may be analysed without context and incorrectly attribute insights.
- As individuals interact in virtual spaces, their movements, speech patterns and other behaviours generate data that could potentially be wholly re-identifying.[45]

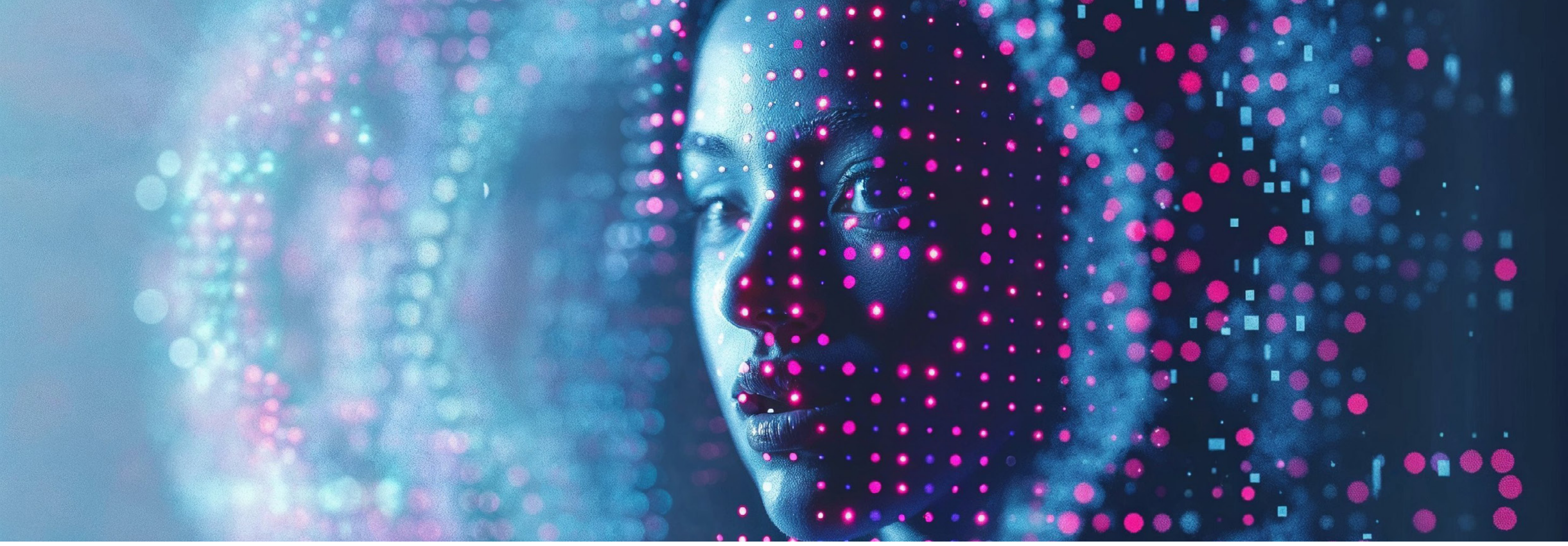
This level of data aggregation and data processing of identifiers[46] and quasi-identifiers[47] could enable profiling people in ways individuals did not intend or anticipate when onboarding to environments or experiences.

Metaverse insight

AI/ML may curate or narrow one's experience – either intentionally or unintentionally – based on an individual's perceived preferences.[48]

While some initial existing and emerging regulation and standards may start to address the privacy, security and processing of this data, stakeholders globally should consider the depth and scale of those instruments to selectively limit and/or restrict data processing for both profiling and re-identification.

As immersive technologies continue to advance, stakeholders should consider how to balance innovation with ethical data practices that respect user privacy and autonomy.



2.3 AI/ML's role in inferred data

With the rise of cloud storage, cloud computing and AI/ML data can now be collected, stored and processed in unprecedented ways, as noted in global dialogue.[49,50,51] For example, a 2020 study suggests that five minutes of VR tracking data can produce "information that can identify a user out of a pool of 511 people with an accuracy of 95.3%", indicating the increasing privacy risks of the metaverse's growing data ecosystem.[52]

However, while the availability and ease of access to data captured via metaverse-supporting technologies may seem ominous, it also empowers individuals and organizations.

TABLE 1 **The value of data processing**

Individual value	Business value
Individuals may use data to: – Track workout routines supported by smart fitness devices capturing real-time data can help define fitness goals, identify physical limitations and challenges – such as balance issues – and modify workouts in real time to create a safer workout. – Capture electroencephalography (EEG) data with external sensors to detect an oncoming migraine and help the individual proactively manage it.	Businesses may use data to: – Offer recommendations based on behaviour and forms of expression, going beyond today's predictive analytics. For example, the design choices an avatar gravitates towards in virtual spaces might infer real-world fashion preferences or socio-cultural affiliations to provide more personalized experiences in both online and offline spaces. – Sample body-based data like pupil dilation, heart rate and brainwaves in a concert setting via AR devices to capture song reactions. AI may infer musical preferences or emotional states during specific song segments to make customized playlists.

Metaverse insight

> Executives, regulators, legislators and society should invest in understanding the power and implications of inferred data[53] – especially as it offers a deeper, more holistic view of both individual users and broader audience segments.

While these examples may initially seem mundane, business executives, regulators, legislators, law enforcement and society should invest in understanding the power and implications of AI/ML models and (inferred) data – especially as it offers a deeper, more holistic view of both individual users and broader audience segments.

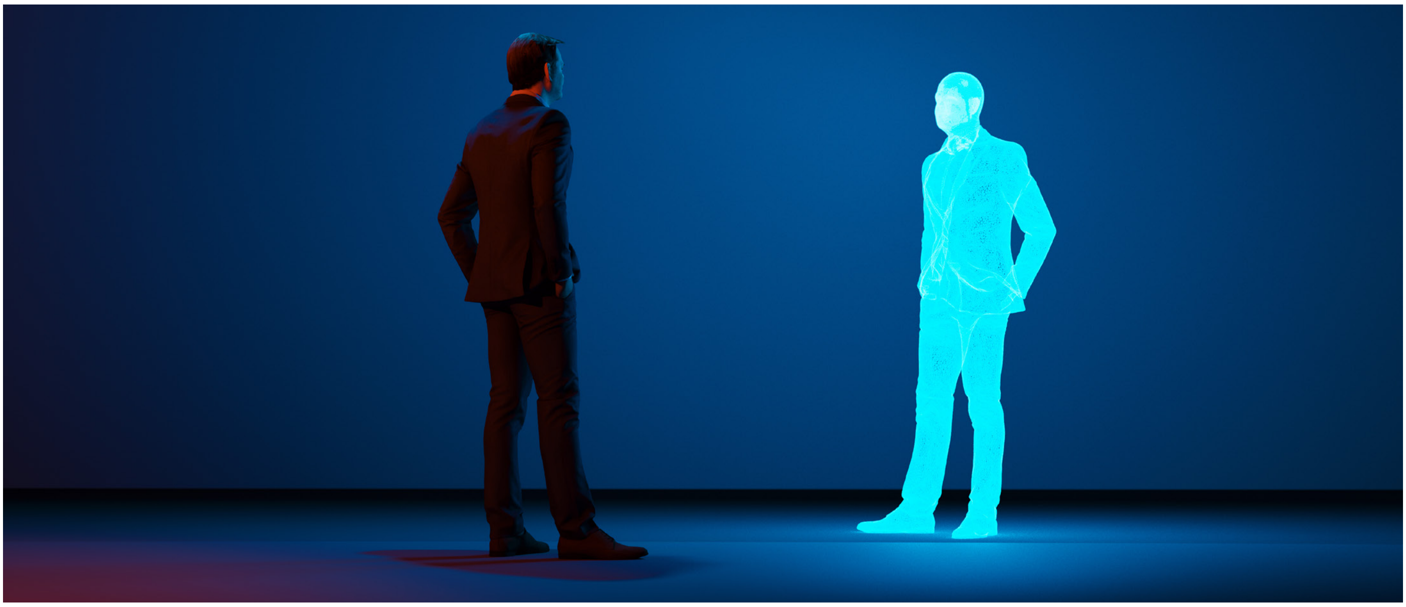
Showcasing the power of inferred data, a research study demonstrated that inferences using neural data can identify and extract an individual's sensitive information. Researchers at the University of California, Berkeley have conducted studies[54] in which they have inserted subliminal messaging into gameplay to probe unconscious brains with suggestion, resulting in successful identification of personally identifiable information (PII).[55]

2.4 New lexicon required to describe metaverse identity

Growing AI/ML capabilities warrant that stakeholders consider the need for an expanded privacy lexicon – building on glossaries such as the one from the International Association of Privacy Professionals (IAPP). Novel terminology may include:

- **Contextual and inferred personal information (CIPI)**: The acknowledgement that an individual's identity is exhibited beyond explicitly provided data points. Instead, an individual's identity is additionally represented by a complex array of behavioural, preferential, and (inferential) data points. Additionally, this information may qualify as personal information (PI),[56] PII, personal health information (PHI)[57] or sensitive personal information (SPI).[58] For example, an individual's habit of online browsing and shopping for kid's clothing through targeted ads is not PI, PII, PHI or SPI – however, when that shopping behaviour becomes contextual, inferred information can be made on the identity of the individual using that device.
- **Known pseudonymity**: 1) a state where an individual operates under a pseudonym that is consistently used across platforms or interactions, making the pseudonym a recognizable marker of their identity without revealing their real name, or 2) a state where a real name is associated with pseudonymity for transparency and traceability.
- **Tangential re-identification (TRD)**: The process of re-identifying an individual by correlating already obfuscated data – such as pseudonyms or other anonymized identifiers – with other types of data, like sensor data or behavioural patterns, to reidentify an individual.

For longevity, technology-agnostic terms, such as the above, must be created to enable stability as technologies evolve.



2.5 Data processing trade-offs

Metaverse insight

Trade-offs lead to the question, "What does the balance of ownership and control look like with regard to (in)voluntary data generation?"[59] For example, an individual can control if they click on a certain link, or navigate to a particular webpage, but they cannot control the data generated from that click or an increase in heart rate when a loud, unexpected add pops up.

The promise of more individualized, responsive and immersive experiences – curated from personal data – must be carefully weighed against the imperative to enable privacy, personal autonomy, trust and safety.

While non-exhaustive, the benefits and risks of inferred data use are detailed in Table 2.

TABLE 2 **Privacy tensions continue**

Benefits of inferred data	Risks of inferred data
The responsible analysis and application of correlational and/or biometric data could provide personal, novel, identity-reinforcing experiences. For example: – Inferred data is beneficial for the prevention of fraud or scoring the risk of fraud occurring, and this use case is generally supported by existing regulations. – Inferred data can enable a more real and nuanced identity-enabling experience – e.g. voice printing may cue a virtual intelligent agent (VIA), like a non-playable character (NPC), in an immersive experience to converse with a regional dialect or accent to make interactions more familiar. – Eye-tracking and associated data can provide real-time insights into an individual's engagement and emotional states, enhancing emotive responses and non-verbal communication for social connections. – Neurotechnologies can offer deeper insights into cognitive processes to unveil unknown qualities or characteristics when paired with other feedback mechanisms, potentially revolutionizing therapeutic interventions. For example, neurofeedback, paired with VR, could allow therapists to discern specific triggers for post-traumatic stress disorder (PTSD), guiding more focused therapies.	Conversely, the collection and handling of such intimate data raises serious privacy concerns, and the potential misuse of information could lead to ethical dilemmas and security threats. – Collected data risks misuse and/or abuse. For example, employment decisions like hiring, promotions or termination could be influenced by inferred data about focus, energy levels or personality traits that unfairly disadvantage certain groups. – Aggregation of personal information could lead to data accumulation sufficient to draw correlations across data sets and re-identify or target individuals unknowingly. For example: – There is a risk that governments could use aggregated inferred data for surveillance, monitoring dissidents or suppressing certain groups without their active consent. – If aggregated inferred data reveals insights about vulnerable populations, they could be targeted for predatory practices or discrimination in housing, lending, etc. – Further, compromised biometric and neuro-data could pose threats to national security, providing new avenues for cyberterrorism or criminal activities. For example: – Criminals could exploit biometric and neurological data leaks to manipulate, blackmail or physically harm individuals.

3 Identification in the metaverse

Digital ID may take new forms in the metaverse, requiring a nuanced approach to credentialled spaces and transactions.

Today's definition of digital identification – digital ID (DID)[60] – stands to be a cornerstone in metaverse identity. Just as passports and driver's licences validate real-world identities, metaverse identity could grant individuals further access to unique experiences, services and transactions.

Like internet interactions today, credentials, verification, authentication and trust[61] anchor online interactions and transactions. As the transition to the metaverse gains momentum, these core identification components will undeniably carry forward, albeit potentially in transformed capacities, as they expand to include aspects of data, representation and digital entities.

3.1 Digital ID and representation

Risks of fraud, impersonation and manipulation take new forms. Voice modifications, video deepfakes and the potential to adapt them compel stakeholders to acknowledge a concerning reality: in the future of the internet, seeing or hearing should not equate to believing. Inappropriate or malicious use of visual data – like that represented by avatars or deepfakes – can:

1. Cause societal disruption
2. Perpetuate stereotypes
3. Promote discrimination
4. Undermine the principles of diversity and inclusivity.

TABLE 3 **Exemplified harms**

Individual manipulation	Impersonation	Fraud
By creating an idealized character or avatar, a nefarious party could catfish or launch a romance scam. This could lead to emotional harm, someone being conned out of money, enabling inappropriate information access or radicalizing the target.	Impersonation of public figures or celebrities could be used to spread misinformation or manipulate followers. Platforms within the metaverse redefine "fame" in many ways, extending the potential for impersonation harms beyond traditional public figures to individuals who might have influence or recognition within digital communities.	Copying or cloning someone else's unique likeness without consent, may enable identity theft and fraud. Further, this could lead to potential harassment, defamation or other forms of abuse should someone's likeness be used inappropriately.

Identity-based crimes are not new. Beyond building on existing frameworks, stakeholders may:

1. Augment a taxonomy of crimes[62] specific to the metaverse – and consequently close identified gaps in current legal frameworks, such as criminalizing harms that occur in online spaces via avatars. For example, harm risk levels may be closely tied to the type of avatars used. Photorealistic avatars could present higher risks of impersonation, while fully customizable stylized avatars could more easily be used for stereotypical or malicious misrepresentation. Either demands clear expectations for recourse and redress.

2. Establish transparent processes for reporting harms like abuse.

3. Extend protections to one's identity and likeness against impersonation, regardless of their level of public recognition. Safeguards like verification systems could help address issues like catfishing, copyright infringement and misinformation spread by impersonation accounts.

4. Implement enforcement thresholds for the community, platform and subsequently law enforcement, impersonation or other violations.

5. Implement platform-level controls and community guidelines around the development and use of avatars.

While preserving free expression, protections should be explored that effectively balance authentic self-expression with safety and integrity, based on the type of avatar and context in question.

Metaverse insight

The level of mitigations around impersonation may vary.[63] For instance, a cartoon elephant avatar might not require the same level of scrutiny as a photorealistic or highly individualized stylized avatar.

3.2 Bifurcating digital ID and representation

Managing identities may involve the intricate processes of creating, maintaining and using a combination of credentials and assets across platforms – potentially in a digital wallet. Ownership and control will influence the management of identities, while ethical considerations should guide how identities are used, shared and represented.

Stakeholders should ponder the strategic value of bifurcating an individual's digital ID from their representative presentation – keeping IDs and forms of representation separate.

While digital assets, like digital entities, might visually depict various layers of an individual's manifested digital self, a distinct boundary between them could reinforce security standards. Such a delineation guarantees that intimate data and IDs remain shielded, separate from the mutable universe of avatars. However, this same delineation may create less transparent environments.

Metaverse insight

Decoupling IDs from digital assets may increase trust and enable new business models.[64]

TABLE 4 **Associating digital assets with digital ID trade-offs**

Option	Linked digital relationships	Bifurcated digital relationships
Description	Enable all forms of digital ID and representation – via digital entities, etc. – to be traceable back to the legal entity.	Limit or entirely disable, an individual or entity's to be linked/traceable back to a singular legal entity.
Pros	– Enables auditing – Promotes transparency	– Enables privacy – Supports voyeuristic, escapism
Cons	– Hinders privacy – Limits voyeuristic, escapism	– Hinders auditing – Reduces transparency

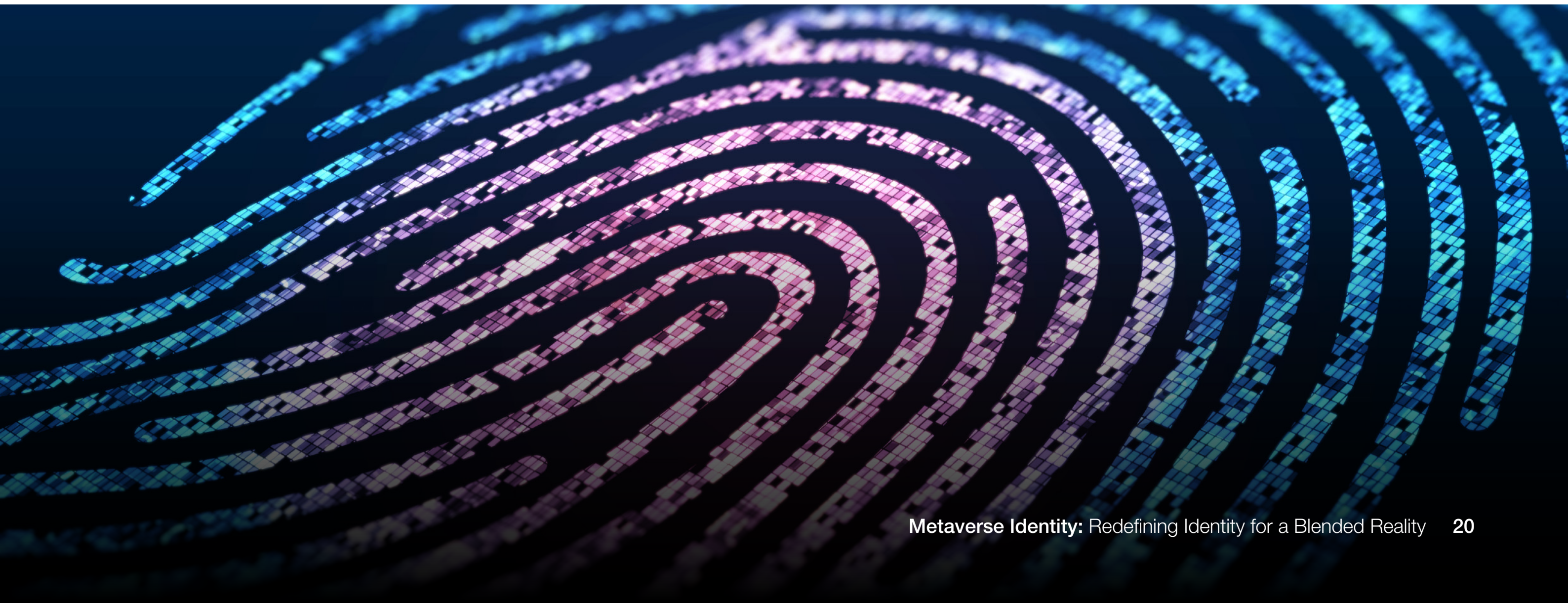
Stakeholders could further consider the following solutions:

1. Imposing hybrid ID structures, such as:

   a. Requiring traceable digital IDs back to a legal entity in environments of high trust, i.e. banking

   b. Not requiring traceability in low-trust environments, i.e. video games

2. Use of trusted digital intermediaries[65] and digital agents[66] when interacting with "unknown" or "untraceable" individuals



3.3 New form factors of digital ID

As the metaverse expands, it will build on existing digital ID frameworks,[67,68,69,70,71,72] and it will raise net-new compelling questions and areas to explore.

TABLE 5 **Possible credential form factors (non-exhaustive)**

Type	
New inferred data-based credentials[73]	The metaverse enables dynamic verification through real-time, inferred data.[74] For example, an individual's behaviours, paired with facial scanning, can be used as ongoing age estimation or "behavioural credentials", effectively making verification an ongoing authentication process based on individual user conduct.
New digital asset/avatar-based credentials[75]	Digital representations could carry credentials. Paired with authenticity checks, a digital asset or avatar's distinctive attributes – whether design, presentation or behaviour – may emerge as a new-age digital signature. However, questions remain: – What meta-data might support the digital signature? – How can the operator be appropriately verified? What should this type of multi-factor authentication look like? – Even if digital assets aren't used as a primary form of identification, might their pairing with other identification mechanisms enable them to be part of an individual's credential and/or verification in digital spaces?
New presentation formats[76]	Identity extends to one's chosen form of representation. These representational forms could serve as a secondary permissions mechanism. For instance, a dragon avatar may only gain access to a "fantasy realm" if it meets certain criteria, like having specific scales or another unique token, thus adding a gating layer. Questions remain: – Should an asset have a degree of likeness to its operator for trust and authentication purposes? – How can asset-based IDs avoid (unintentional) profiling, bias or discrimination? – How can asset-based credentials be harmonized across multiple, potentially competing platforms? How should metaverse identity components be standardized?

3.4 Know-your-customer in the metaverse

A pivotal factor in fostering trust will be identity verification conducted by independent bodies.[77] Determining who these bodies would be, and establishing their credibility, will be critical. These independent entities could be responsible for verifying the authenticity of users' identities, ensuring the security and accuracy of transactions and providing a layer of trust that is essential for meaningful interactions and exchanges.

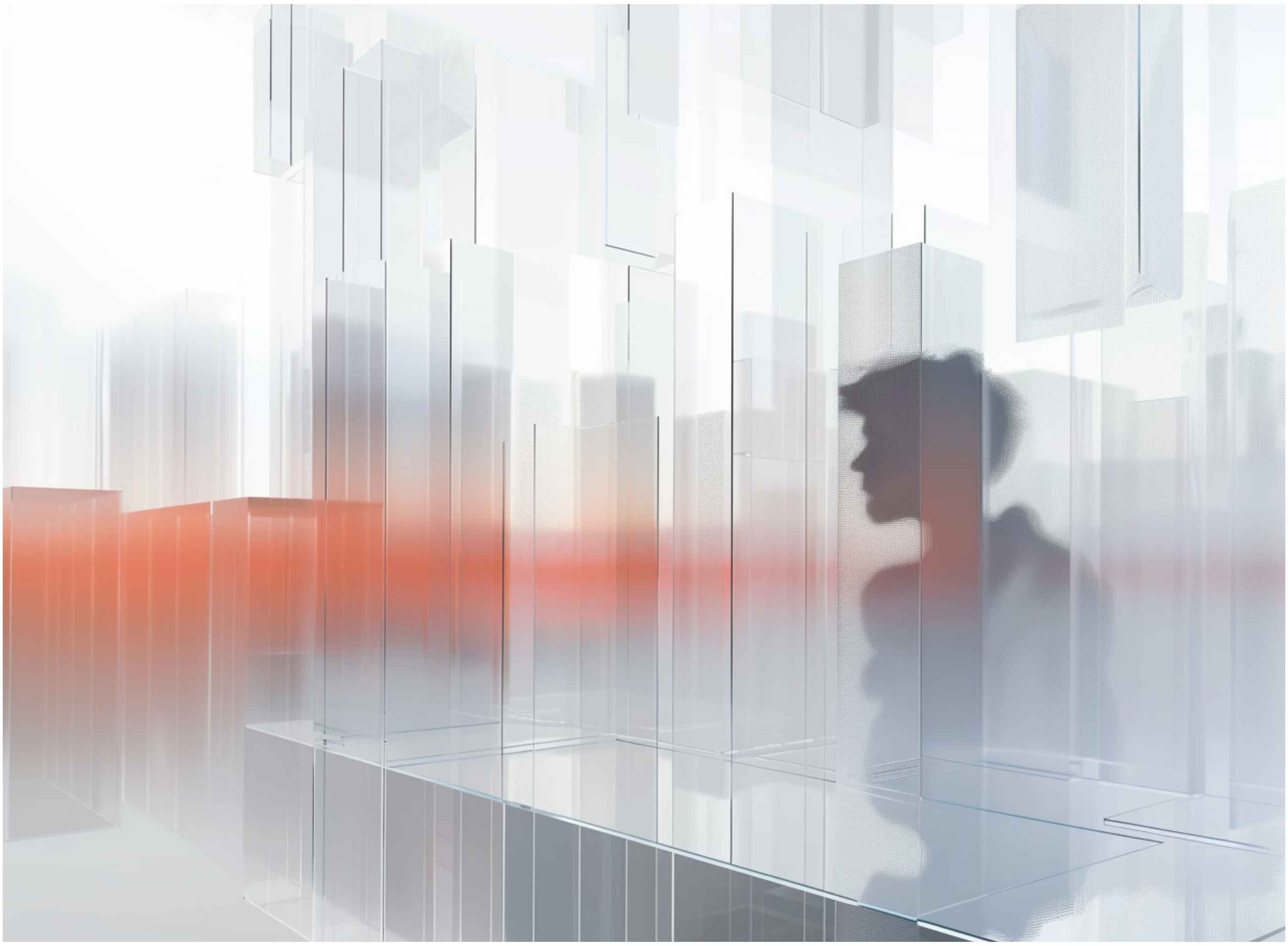
To reinforce trust, stakeholders should consider the evolution of know-your-customer (KYC).[78]

- **Might KYC adapt for body-based[79] identity?** Instead of traditional verification methods, it may become commonplace to recognize a person's unique movement patterns or digital asset-specific credentials as markers of identity.

- **Might KYC adapt for interoperable spaces?** If participants are empowered to move across platforms and spaces with their avatars, digital wallets and associated money and objects,[80] what level of information will need to be shared across experiences?

- **Might KYC adapt for representation?** With identity expanding to include digital assets, stakeholders may set the criteria for what representations are appropriate to use as KYC mechanisms, based on the nature and purpose of various virtual environments.

- **Might KYC incorporate visual verification indicators?** A visual verification system – and supporting assistive accessibility applications – could be adopted to enhance trust and transparency in immersive environments. This could manifest as distinct colour outlines on an avatar, indicating that the user is the primary human user, a guest user, a virtual intelligent agent, NPC, etc., and has completed a KYC verification process. This visual cue could help users easily identify and trust verified identities, promoting a safer interaction environment.



3.5 Requirement for a nuanced digital identity approach

As the metaverse matures, it could be envisioned as a public utility akin to the internet's role today. Therefore, it's important to design a digital identity approach that treats the metaverse as such.

Metaverse insight

Penalizing individuals who don't wish to create digital identity profiles[81] – such as by not wishing to create social media profiles – can augment the digital divide.[82]

For example, a school's group that is only hosted on a virtual platform may prevent a parent from participating in their child's school functions if that parent does not wish to create an account on that platform – either for privacy reasons or otherwise.

When designing public and private spaces, stakeholders should remember that mandatory credential-based access limits accessibility. Stakeholders should additionally consider how to create inclusive spaces for the following individuals who:

- Are unidentified or under-identified[83] and may be put at risk by creating a digital footprint[84]
- Cannot access appropriate technologies or are slow to adopt technologies
- Are, by choice, fully offline or partially offline and wish to engage passively – as spectators or consumers of mediated realities.

4

Representation through metaverse identity

Identity goes beyond pixels, emphasizing the need for authentic and inclusive representation to create deeper human connection.

In both 2D and 3D – ranging from AR to VR, the notion of "representation" is not just about pixels and graphics; it's a reflection of societal values, inclusivity and the human desire for authenticity.

Getting representation right in these digital realms is pivotal because it directly impacts how individuals perceive themselves and others in real-world and digital environments.

- Mistakes or biases in representation can perpetuate real-world stereotypes, marginalize groups, create monocultures or diminish presence and belonging.[85]
- Conversely, accurate and inclusive representation can promote empathy, broaden perspectives and elevate the metaverse from a buzzword to a transformative space for human connection and understanding.
- As users build and curate metaverse identities, it will be critical to define appropriate safeguards to minimize risks such as impersonation and avoid empowering bad actors to escape accountability.

Representation – through cultural norms, etiquette, physical presentation and expression – takes on profound significance across public and private spaces. This is further emphasized by the blending of digital and physical worlds and the introduction of digital entities.

4.1 Presentation through multiple identities and spaces

The ability to adopt multiple identities tailored to different contextual situations reflects the multifaceted nature of human identity.

TABLE 6 **Examples of identity types (non-exhaustive)**

Category	Personal identity[86]	Public identity[87]	Social identity[88]	Professional identity[89]
Description	Personal identities are those that are formed when no monitoring occurs. This includes the composition of an individual's true self and their unhindered thoughts, feelings and choices.	Public identities are those that are displayed under observation. This includes only the qualities or characteristics that an individual wishes to display within a particular context.	Social identities are a form of public identity but are contextualized for socialization within specific groups.	Professional identities are a form of public identity but are contextualized for professional environments.
Design considerations	– Design diverse spaces and activities that can be tailored to align with personal values, interests and styles. – Enable rich forms of expression through avatars, creative tools and communication options. – Allow user reputations, histories and relationships to selectively carry over across experiences through interoperable design.	– Collaborate with diverse communities relevant to the public space being created. – Consider how public norms evolve and design systems that can adapt. – Address challenges of privacy, laws/regulations and socially accepted behaviour to govern public spaces. Conduct moderation is key.	– Design with the social group. Ensure design promotes inclusivity. – Encourage community ownership, moderation and a sense of belonging and trust.	– Design with professional groups, organizations and industry-specific bodies. – Consider the future of work, and accessibility for all levels professionally and geographically. – Design should respect autonomy and individuality while preserving privacy and security. – Privacy compliance and security choices should be regularly reviewed, updated and hardened for identity-based data. – Diverse needs and expectations, along with user-based control should be paramount.

To enable navigating multiple identities in a blended digital/physical world:

- Platforms and applications should provide granular and flexible ways of choosing various presentations of identities depending on which one the audience wants to project.
- Stakeholders should invest in developing harm and impact models that further explore the multi-faceted nature of identity types.
- Stakeholders should invest in understanding how to enable an individual to create, operationalize and switch between these various identities in digital spaces while also potentially enabling a link to a physical, tangible person for purposes of safety and legality.

Designing for multiple identities across public and private spaces is a human-first approach.[90,91] Harmonizing the autonomy of personal identity exploration with the integrity of community standards helps create digital personae that are authentic extensions of oneself.

4.2 Representation across realities

Metaverse insight

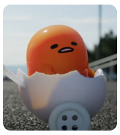
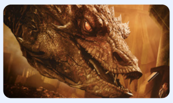
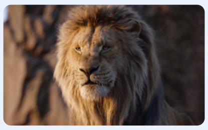
Avatars and other related digital assets must be thoughtfully designed to avoid exclusion or limitation due to a lack of options for cultural representation, body type, age expression, cultural artifacts, etc.[92]

Identity is often constrained by societal norms and physical reality limitations. However, the future of the internet offers a flexible, fluid and dynamic space where identity can be constructed, moulded and changed digitally to suit an individual's preferred presentation and expression of self.

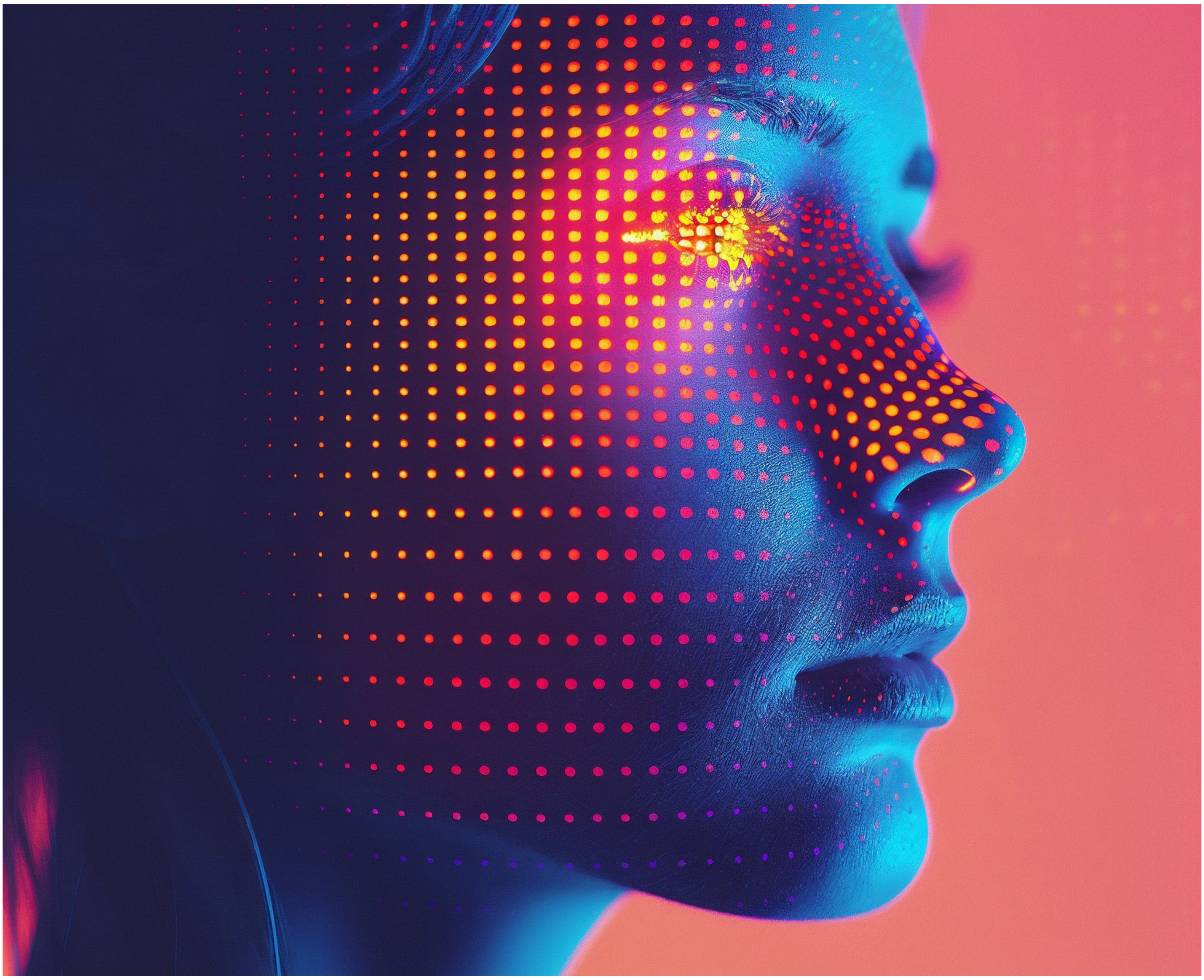
The internet is enabling individuals to engage in novel, digitally enhanced ways. For example, starting in early 2015, Snapchat enabled individuals to enhance themselves with photo and video filters.[93] Whether in VR or in a more blended reality through AR and MR – where a physical person can be superimposed with computer generated graphics, text, animations, accessories and more – the future of the internet will enable means for personal representation.

Representation can be photo-real or entirely stylized, with high levels of variability.

TABLE 7 **Example of a spectrum of representations (non-exhaustive)**

	Fantastical		Realistic	
	Non-human	Humanoid	Non-human	Human
Stylized	Spyro the Dragon Insomniac Games 	The Legend of Zelda – Links Awakening Nintendo 	Gudetama: An Eggcellent Adventure Netflix 	ReadyPlayerMe Avatars
Photo-real	Smaug – The Hobbit: The Desolation of Smaug MGM 	Ronal – Avatar: The Way of Water 20th Century Fox 	The Lion King Disney 	Meta – Codec Avatars – Mark Zuckerberg[94] (courtesy of Lex Fridman interview)

This variability requires additional governance considerations when curating experiences. Governance considerations could include standards and policies to community guidelines that dictate acceptable representation and forms of expression etc. – ranging from fantastical to realistic.



4.3 Dysmorphia and depersonalization-derealization

The future will enable more AR and MR through avatars, filters and associated accessorizing digital assets. These may be a common digital extension of oneself, allowing individuals to creatively explore and express various facets of their identity – some of which may not be possible in the physical world. A lack of representation or supportive communities where this type of creative exploration may take place may cause harm. Additionally, unfettered augmentation[95] may incidentally promote reality dysmorphia and/or depersonalization-derealization disorder (DPDR).[96]

Recent research in DPDR[97] has shown feelings of detachment in VR, where technology blurs the lines between objective reality and virtual reality or boundaries between a sense of self and avatar embodiment. Some individuals might find it difficult to integrate their online persona(s) with their real-world self, leading to struggles in self-perception and understanding. Virtual environments might further reinforce or aggravate existing feelings of unreality, contributing to a cycle that further entrenches the disorder.

Recent discourse has shown[98] that AR "beautification" filters may be promoting body dysmorphia. While such identity presentation options are meant to provide diversion and entertainment, they may be exacerbating DPDR-related issues. Further research is needed to fully understand the relationship between DPDR and virtual environments, particularly as technology evolves and becomes more immersive.

5

Digital entities in the metaverse

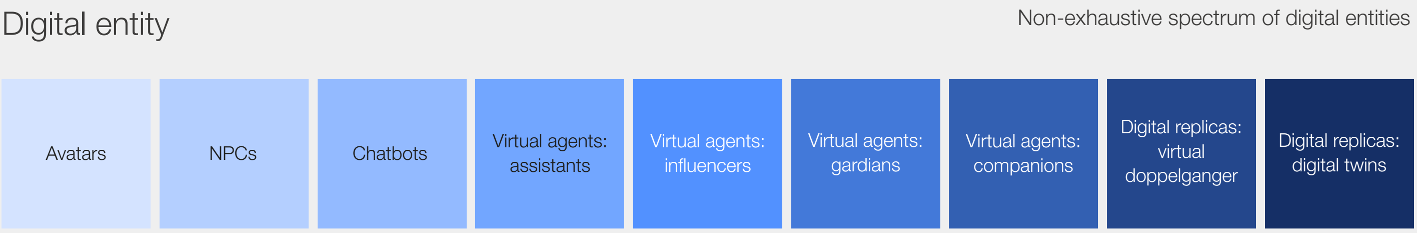
Representation, data and ID are not limited to humans; digital entities will play a role in the future of the internet.

Digital entities refer to a broad spectrum of digital representations and interactive embodiments within digital computing environments.

Metaverse insight

Digital entities may represent humans, objects, systems or abstract concepts, and are capable of varying degrees of interaction, autonomy and behaviour within digital experiences.

FIGURE 3 **Digital entity**

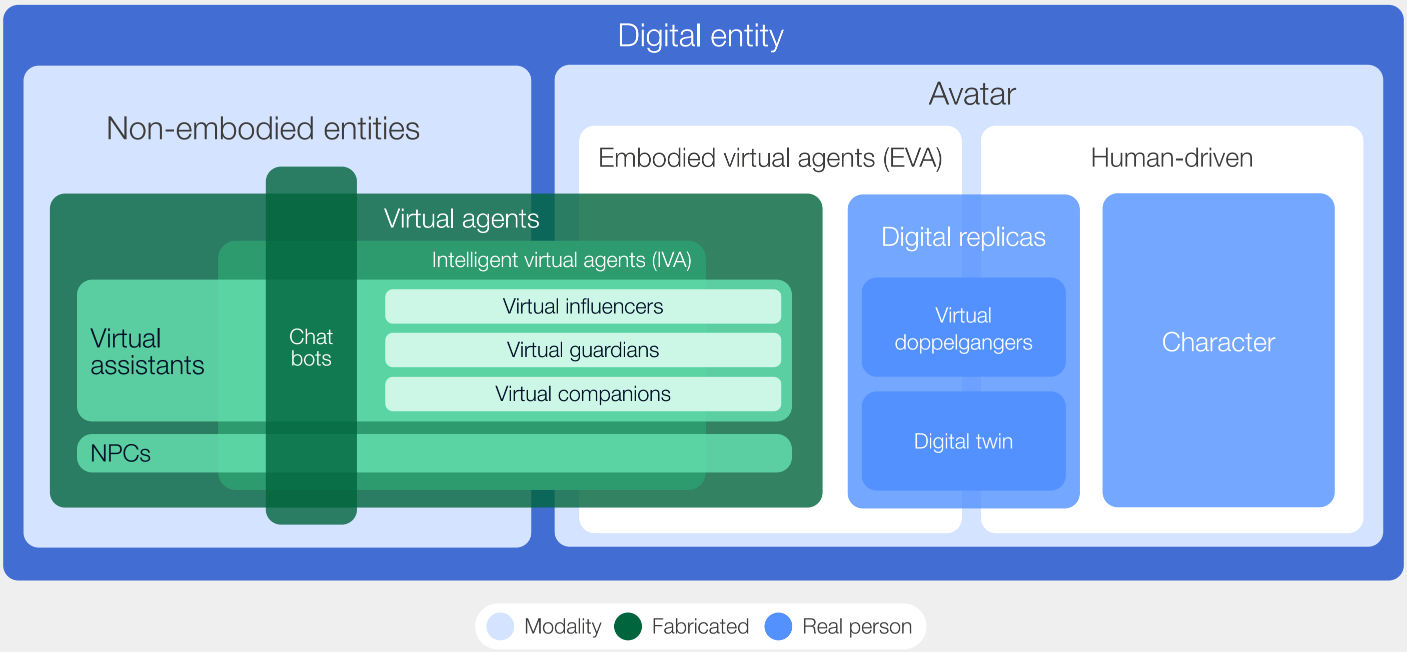

Digital entity
Non-exhaustive spectrum of digital entities
Avatars
NPCs
Chatbots
Virtual agents: assistants
Virtual agents: influencers
Virtual agents: gardians
Virtual agents: companions
Digital replicas: virtual doppelganger
Digital replicas: digital twins

5.1 What are digital entities?

Digital entities broaden the concept of identity beyond physical individuals. Digital entities encompass a range from simple text-based chatbots to complex, human-like avatars and digital replicas like doppelgangers and digital twins.

Digital entities may represent humans via avatars, objects via digital twins and third parties via chatbots. Each is capable of varying degrees of interaction, autonomy and behaviour within digital experiences. They are capable of mimicking human communication and may be used as sales assistants, corporate trainers, social media influencers and more.

FIGURE 4 **Digital entity relationships**



Note: While various terminology is used across academia, industry and identity discourse, this figure represents the cascading relationships between terminology. It is not intended to be exhaustive.

Digital entities are used today:

- Companies are deploying digital entities across organizations in business-to-customer (B2C) and business-to-business (B2B) functions, leading to increased sales conversions, better customer retention, and lead generation.[99]
- Individuals are employing digital entities to provide emotional engagement[100] and reduce friction in daily activities[101,102] and benefit from anthropomorphic[103] agents.

TABLE 8 **Digital entities**

Description	Example
Virtual agents: These may range from fully autonomous to pre-programmed and may be represented in embodied[104] or non-embodied forms.	The modality of virtual agents may be embodied via an avatar or may not contain a visual component at all. – **Virtual influencers**: Unlike human influencers, they are digitally generated. For example, @lilmiquela[105] is an Instagram influencer with over 3 million followers, Miquela posts pictures, endorses products and interacts with followers, but she's entirely generated. Her identity, though virtual, influences real-world fashion and lifestyle trends. – **Virtual guardians**[106]: Think of a babysitter or a bodyguard. Virtual guardians are entities that have defined responsibilities, such as interpreting aggressive behaviour or alerting individuals to perceived dangers. Virtual guardians can also offer guidance to help inform users of potential risky interactions/transactions. – **Virtual companions**: Consider an entity that offers personalized companionship. This digital entity might reminisce about old songs, discuss books or simply chat, providing comfort and companionship. Anima provides a platform to enable this type of interaction. – **Virtual assistants**: Virtual assistants are software applications designed to assist users in performing tasks or services, either online or offline, by interpreting and executing commands given by an individual. Think of Apple's Siri or Amazon's Alexa but that can be augmented with a human face and gestures.[107] – **NPCs**: This refers to a character within a game or a virtual environment that is not controlled by an individual but rather by a game or environment's programming.
Character:	A character[108] represents a role or persona that can be assumed by, or assigned to, an individual. A character represents a proxy for the individual in a digital experience like a video game or social experience. Characters typically have pre-defined traits, characteristics, stories, etc.
Digital replicas:	**Digital twin**: In industrial contexts, digital twins are copies of physical assets that can be connected to digital spaces via sensors – such as a building, machine or manufacturing line. This is intended to be a one-to-one, sensor-driven version of oneself or one's anatomy. Consider a replica of a human heart – while this isn't a complete doppelganger of oneself, it is a digital replica of a physical asset, machine or live human system. This heart replica may be used for near-real-time information and representation of an individual. **Virtual doppelganger**: These are intended to be proxies or close replications of holistic people. This may be an avatar that is a "digital twin-like" replica of an individual – either through photorealism, mannerisms or knowledge expertise in a particular field. Virtual doppelgangers may provide value through use cases such as: – **Health monitoring**: A person can see potential health outcomes over time by inputting an individual's daily nutrition and exercise habits into the doppelganger's simulated environment. Similarly, an athlete may train with their virtual doppelganger to test new techniques or strategies, receiving data-driven feedback on performance, energy use and potential for injury. – **Fashion try-ons**: Before purchasing a new outfit online, an individual uses their virtual doppelganger to try on clothes, ensuring they fit and look right before making a purchase. – **Teaching**: A professor trains a virtual doppelganger on her lectures to be available on-demand to answer ad-hoc questions and provide 24/7 lecture availability to meet student needs for alternative learning hours. – **Immersion**: A professor immerses students in art history by using replicas of famous artists. Students may virtually stroll through historically accurate streets, interacting with artists like Botticelli and Michelangelo, witnessing first-hand the artistic techniques and cultural nuances that defined the period.

Child insight

Children – who lack autonomy and legal ability to navigate digital interactions – may benefit from digital guardians[109] who can function as a guardrail.

New digital entity business models may be augmented using generative AI tools; however, care should be taken in initiatives that involve digital entities. Research has shown that entities may:

- Pose significant risks when not understood by end-users, resulting in over-trust[110]
- Be exploited by adversaries[111] for manipulation and misinformation or be used for predatory sales or advertising.[112]

The promise and the peril of digital entities call for a human-first design approach to ensure responsible, ethical and trustworthy use of the technology and to ensure their representation in metaverse identity is genuine and inclusive.

5.2 Responsible digital entity design

Delving into various roles and applications of digital entities – from virtual assistants and companions to influencers and doppelgangers – it becomes clear that they are more than just lines of code or graphical representations; they are entities that interact with, influence and, in the case of avatars, can represent individuals.

These digital entities may be managed either directly via human control or orchestrated through AI. This requires special design considerations across:

1. **The desired levels of autonomy and control** the creator wishes to provide or maintain over the digital entity – either via pre-programming or degree of output variability.
2. **The expressive capabilities the digital entity possesses** – across visual representation, actions and behaviours, conversational abilities and emotive capabilities.

Digital entity's capability for emotional engagement, customization and scalability presents enormous opportunities but also comes with ethical considerations.

5.2.1 Designing with representation, inclusivity and access in mind

Stakeholders must explore representational aspects in depth, examining how to responsibly assimilate digital entities into evolving notions of identity across blended physical and digital spaces.

Metaverse insight

> Representational design choices extend to the design of digital entities[113] – from embodied virtual agents to non-embodied virtual assistants.

Ecosystems with digital entities should represent a wide spectrum of ages, genders, ethnicities and even abilities. This requires an intersectional approach that goes beyond just skin-deep appearances. For instance, the way a digital entity communicates – its language, tone and gestures – should be diverse and inclusive.

Moreover, to bring the benefits of digital entities to the widest audience, stakeholders must consider the technology access gap.[114] The lack of reasonable internet access, paired with inaccessible enabling hardware and software, may prevent individuals from using digital entities such as virtual agents in the form of guardians and companions. Stakeholders should consider how to create accessible guardians and companions that do not require continual internet access.

5.2.2 Designing digital entities with AI governance in mind

Metaverse insight

> Responsible AI is a critical centrepiece to enabling digital entities in the metaverse.[115]

Many organizations[116,117,118,119] and initiatives[120,121] have been formed to understand what responsible AI looks like. This is increasingly important given that digital entities are becoming ever more present in blended physical/digital worlds, from AI-driven customer service agents to using generative AI models to give voice to NPCs.

This requires that stakeholders further enable AI governance structures to consider how to:

1. Make decisions based on responsible AI principles
2. Identify risks and necessary policies to provide adequate oversight and control of digital entities
3. Manage use case selection – determining if, when, where and how digital entities are deployed
4. Develop, monitor and maintain underlying AI models that may be directing the actions of digital entities.

Additionally, stakeholders must address the public's ongoing concerns of transparency and verification. Mechanisms to disclose digital entities and authenticate their intended application and capacity are critical for both trustworthy interactions and successful assimilation. For example, users should be clearly aware when they are interacting with an AI-powered digital entity, as well as what data processing that entity may be facilitating.

5.2.3 Authenticity of digital entities

Given a digital entity's ability to interact, engage and even influence within blended digital and physical environments, chatbots, human-driven avatars and AI-driven virtual agents should also be given representational consideration to promote authenticity.

For example, influencers play a central role in advertising globally, with brands estimated to have invested up to $15 billion in influencer marketing by the end of 2022.[122] The appeal for companies to employ influencers lies in the creator's personal blend of authenticity, ability to connect with others and aspirational allure. Moreover, this meets a brand's desire to develop timely, authentic branding, imaging and messaging that aligns with company policy.

The flexibility of choice when creating digital entities and the ease of digital duplication raise critical questions around positive and controversial representation.

TABLE 9 **Representation examples**

Positive representation	Controversial representation
Successful virtual influencers: Lil Miquela: An American virtual influencer, with 2.8 million Instagram followers, known for her music, style and activism. Lil Miquela has collaborated with real-world brands and musicians and has even released her own music, topping Spotify charts. During the pandemic, Bloomberg reported that Lil Miquela charged $8,500 per sponsored post.[123] Lu do Magalu: A 3D virtual influencer and digital specialist at Brazilian retail giant Magazine Luiza, with 6.5 million followers on Instagram. Lu do Magalu primarily engages with audiences through unboxing videos, product reviews and software tips. She has been particularly successful in Brazil. K/DA: A virtual K-pop girl group created by Riot Games, the company behind the popular online game League of Legends. The band comprises four themed versions of League of Legends characters: Ahri, Akali, Evelynn and Kai'Sa. Real-world artists voice each of these virtual characters.[124]	**FN Meka**: Capitol Records signed the virtual influencer FN Meka, developed by a start-up called Factory New and voiced by a real artist, to a record deal. Shortly after, Capitol Records shelved the project, citing criticism and backlash from black music industry professionals who said the influencer was fashioned out of reductive stereotypes.[125]

This opens many tangible and philosophical questions about the expressive and representational nature of digital entities' roles, responsibilities and expectations.

5.3 Accountability and digital entities

As blended and physical worlds come together and the role of digital entities becomes more commonplace, stakeholders must consider accountability of:

- Proving personhood
- Actions occurring around digital entities.

Standards, guidance and regulation, such as the European Union's AI Act, will play a critical role.

Metaverse insight

In the metaverse, accountability is a two-way responsibility – relating to answerability, culpability and liability of actions.[126]

While an individual should remain vigilant of their personal interactions with digital entities, platforms carry the responsibility to create safe environments with trusted digital entities.[127]

5.3.1 Accountability of proving personhood

The ability to manipulate or create misinformation through digital entities – such as chatbots[128] and photoreal avatars[129] – raises ethical and security concerns. These challenges underscore the importance of robust mechanisms to verify and validate identities. One such mechanism is the ability to prove personhood.

Digital entities should have the means to disclose whether it is human-driven or AI-driven.[130] If human-driven, individuals should be provided with the assurance that the individual behind the entity is the person being presented and not someone else without permission.[131]

This concept is vital for maintaining integrity, trust, and accountability and reinforcing recourse and redressability.

5.3.2 Accountability and digital entities

While digital entities can offer innovative interactions and functionalities within the metaverse, they may commit real-world harms. Determining what pass-through liability should translate from the digital entity to the associated physical individual or company is essential. Proactive measures may require stakeholders to:

- Develop and implement frameworks for liability should a digital entity commit a harm, e.g. if a person's digital replica voices slander in a public setting.
- Develop mechanisms that unambiguously link digital entities back to their operator and/or creator for law enforcement responses.
- Capture actions performed by AI-driven entities to enable recourse and redress.

Stakeholders should further consider that AI-driven digital entity operations should:

1. Be transparent and easily identifiable to other users to maintain a level of trust and safety
2. Apply clear labelling of entities, perhaps through visual indicators
3. Provide accessible and clear knowledge bases to inform users of the capabilities and limitations of AI-driven entities and set expectations for interactions and reliability.

6 Education is key

Building identity literacy across digital rights, management and security challenges is essential for safely navigating the metaverse.

Metaverse insight

Individuals should stay informed regarding the technical components of metaverse identity,[132] how it can be used and the resulting consequences of how an identity is used.

As metaverse identity evolves, integrating not just digital IDs but also a complex array of data and new form-factors of credentials, the challenge of keeping individuals informed becomes a monumental task that requires multistakeholder investment and support.

While not all individuals will need the domain expertise of a lawyer or a data scientist, there is an opportunity for all individuals to learn and take accountability for their own identity. Just like in the physical landscape today, individuals are expected to stay aware of legal and ethical considerations that surround their existence.

Stakeholders across the board – governments, platforms and civil society – have a vested interest in ensuring comprehensive education and awareness programmes are in place.

- Clear guidelines and educational resources should be developed to help people understand the scope and limits of their digital rights, the technologies driving their virtual identities and the responsibilities that come with participating in a digital society.
- Awareness of potential harms within the metaverse, such as digital fraud, harassment or exposure to inappropriate content, is crucial to ensure individuals are well-informed and prepared.
- Educating individuals on how to defend against social engineering attacks aimed at stealing their virtual identity, money and/or digital assets is paramount. Simple, clear and actionable advice on recognizing phishing attempts, securing personal information and what steps to take if they suspect they're under attack or have been compromised should be part of the education curriculum.
- Interactive tutorials, easily accessible frequently asked questions and real-world analogies can help demystify complex topics.
- Considering the global reach of the metaverse, these educational materials must be accessible, multilingual and culturally sensitive to effectively reach a broad audience.

Child insight

While parental involvement can contribute to a child's metaverse literacy, there is increased responsibility for stakeholders – platforms and governments alike – to prioritize the digital education of children.[133]

Conclusion

The discussions above underscore the centrality – and complexity – of identity in the metaverse. Identity is not a singular construct; it encapsulates data, representation and identification across analogue humans and digital entities.

The stakes are high. As people navigate this new terrain, their sense of belonging, privacy, security and trust will be anchored to their digital identities. A successful transition to this new metaverse era requires more than just immersive hardware and software; it demands a concerted effort from stakeholders globally to rethink the notions of identity beyond a digital ID or identity access and management system.

Policy-makers, academics, regulators, law enforcement and design teams must rally together to ensure that this new realm is constructed on the tenets of equality, inclusivity, accessibility, authenticity and trust. Without trust, the vast potential of this space risks being undermined.

The metaverse could be fertile ground for powerful manipulative tactics, putting the onus on the global community to establish robust frameworks that not only facilitate the growth of the metaverse but also safeguard its integrity. As the metaverse evolves, this community issues a clarion call: the journey ahead should prioritize human-first values, ensuring a metaverse that is not only economically prosperous but also a beacon of human rights, equality and sustainability.

Contributors

World Economic Forum

Daniel Dobrygowski
Head, Governance and Trust, Centre for the Fourth Industrial Revolution Digital Technologies

Judith Espinoza
Specialist, Metaverse Governance

Cathy Li
Head, AI, Data and Metaverse, Centre for the Fourth Industrial Revolution; Member of the Executive Committee

Dylan Reim
Lead, Metaverse Governance

Accenture

Matt Price
Fellow, Metaverse Governance, Responsible Innovation Strategy Manager, Responsible Innovation Group

Anna Schilling
Fellow, Metaverse Governance, Data & AI Value Strategy, Responsible AI Group

David Treat
Senior Managing Director, Innovation Incubation Group Lead

Kathryn White
Executive Fellow, Centre for the Fourth Industrial Revolution; Principle Director, Responsible Innovation

The project team would also like to extend special appreciation to Aiden Slavin, whose dedication to and expertise on identity issues significantly contributed to the development of this report.

Acknowledgements

Steering Committee Members

Sincere appreciation is extended to the following steering committee members, who spent numerous hours providing critical input and feedback to the drafts. Their diverse insights are fundamental to the success of this work.

Judson Althoff
Chief Commercial Officer, Microsoft

Jeremy Bailenson
Thomas More Storke Professor of Communication, Stanford University

Stephanie Burns
Senior Vice-President and General Counsel, Sony

Adam Caplan
Senior Vice-President, Emerging Technology, Salesforce

Inhyok Cha
Group Chief Digital Officer, CJ Group, Chief Executive Officer, CJ Olivenetworks

Phil Chen
Chief Decentralized Officer, HTC-VIA

Rob Sherman
Deputy Chief Privacy Officer, Meta

Julia Goldin
Chief Product and Marketing Officer, LEGO Group

Julie Inman Grant
eSafety Commissioner, Office of the eSafety Commissioner, Australia

Marwan Bin Haidar
Executive Vice-President, Innovation and the Future, Dubai Electricity and Water Authority (DEWA)

Royce Wee
Director, Department of Communications and Connectivity, and Department of Data Protection, NEOM Authority.

Huda Al Hashimi
Deputy Minister, Cabinet Affairs for Strategic Affairs, Office of the Prime Minister of the United Arab Emirates

Brittan Heller
Fellow, Digital Forensics Research Lab, The Atlantic Council

Paula Ingabire
Minister of Information Communication Technology and Innovation, Government of Rwanda

Peggy Johnson
Chief Executive Officer, Magic Leap

Nuala O'Connor
Senior Vice-President and Chief Counsel, Digital Citizenship, Walmart

Tony Parisi
Chief Product Officer, Lamina1

Philip Rosedale
Co-Founder, High Fidelity

Yat Siu
Co-Founder and Executive Chairman, Animoca Brands

Hugo Swart
Vice-President and General Manager, XR, Qualcomm

Artur Sychov
Founder and Chief Executive Officer, Somnium Space

Kent Walker
President, Global Affairs and Chief Legal Officer, Google

Wilson White
Vice-President, Government Affairs and Public Policy, Google

Working group members

This insight report is a combined effort based on numerous interviews, discussions, workshops and research. The opinions expressed herein do not necessarily reflect the views of the individuals or organizations involved in the project listed below.

Sincere appreciation is extended to the following working group members, who spent numerous hours providing critical input and feedback on the drafts. Their diverse insights are fundamental to the success of this work.

Joe Abi Akl
Chief Corporate Development Officer and Managing Director of Xsight Future Solutions, Majid Al Futtaim Holding

Seokhyun Elliott Ahn
Vice-President, DT Executive Director, CDO Office and Chief Strategy Officer, CJ ONS

Anju Ahuja
Vice-President, Product Strategy and Insights, CableLabs

Saeed Aldhaheri
Director, Center for Futures Studies, University of Dubai

Flavia Alves
Head, International Institutions Relations, Meta Platforms

Ahmed Saeed Abdulla Alshami
Head, AI Systems and Services Development Team, General-Directorate, Ministry of the Interior, United Arab Emirates, United Arab Emirates Government

Maurizio Arseni
Freelance Tech Journalist

Yoni Assia
Chief Executive Officer, eToro

Frank Badalamenti
Partner, PwC Americas

Moritz Baier-Lentz
Partner and Head of Gaming & Interactive Media, Lightspeed Venture Partners

Jeremy Bailenson
Professor, Stanford University

Avi Bar-Zeev
Founder and Chief Technology Officer, RealityPrime

Luna Bianchi
Advocacy Officer, Privacy Network

Doreen Bogdan
Director, Telecommunication Development Bureau, International Telecommunication Union (ITU)

Gustavo Borges
Professor of Human Rights and Social Media, Department of Human Rights, University of the Extreme South of Santa Catarina (UNESC)

Sebastien Borget
Chief Operations Officer and Co-Founder, The Sandbox

Marine Boulot
Vice-President, Public Relations and Communications, Improbable Worlds

Mahmut Boz
Head, Anticipatory Regulation and Regulatory Experimentation, NEOM

Gareth Burkhill-Howarth
Global Data Protection Officer, WPP

Jehangir Byramji
Emerging Technology and Innovation, Lloyds Banking Group

Marquis Cabrera
Chairman and Chief Executive Officer, Stat Zero

Adam Caplan
Senior Vice-President, Emerging Technology, Salesforce

Isaac Castro
Co-Chief Executive Officer and Co-Founder, Emerge

Achyut Chandra
Senior Manager and Global Lead, OI and Technology Venturing, O/o CTO, HCL Technologies

Pearly Chen
Vice-President, HTC-VIA

Phil Chen
Chief Decentralization Officer, HTC-VIA

Magda Cocco
Head, Practice Partner Information, Communication and Technology, Vieira de Almeida & Associados

Anna Maria Collard
Senior Vice-President, Content Strategy and Evangelist Africa, Knowbe4 Africa

Sandra Cortesi
Director, Youth and Media, Berkman Klein Center for Internet and Society, Harvard University

Sadie Creese
Professor of Cybersecurity, University of Oxford

William Cutler
Head, Tech Policy and Deputy to UK Tech Envoy, United Kingdom Foreign, Commonwealth and Development Office

Nighat Dad
Executive Director, Digital Rights Foundation

Julie Dawson
Chief Policy and Regulatory Officer, Yoti

Ellysse Dick
Policy Manager, Reality Labs

Eileen Donahoe
Executive Director, Global Digital Policy Incubator, Stanford

Sarah Kate Ellis
President and Chief Executive Officer, GLAAD

Liv Erickson
Innovation Ecosystem Development Lead, Mozilla

Maureen Fan
Co-Founder and Chief Executive Officer, Baobab

Nita Farahany
Robinson O. Everett Professor of Law and Philosophy; Director, Duke Science and Society, Duke University

Ellysse Dick
Policy Director, Reality Labs

Steven Feldstein
Senior Fellow, Democracy, Conflict and Governance Program, Carnegie Endowment for International Peace

Jordan Fieulleteau
Policy Manager, Reality Labs

Francesca Ginexi
Public Policy Manager, Privacy Legislation, Meta Platforms

Inbal Goldberger
Vice-President of Trust and Safety, ActiveFence

Paula Gomes Freire
Managing Partner, Vieira de Almeida & Associados

Patrick Grady
Editor of Metaverse EU, Tech Lead at Fourtold

Ashraf Hamed
Value Proposition Innovation and Pioneering, SAP

Cortney Harding
Chief Executive Officer, Friends with Holograms

Susie Hargreaves
Chief Executive Officer, Internet Watch Foundation (IWF)

Huda Al Hashimi
Assistant Director-General, Strategy and Innovation, Ministry of Cabinet Affairs and Future

Mohamed Heikal
Head, Corporate Development, Majid Al Futtaim Holding

Vera Heitmann
Leader, Digital and Growth, Public Affairs, IKEA

Brittan Heller
Fellow, The Atlantic Council

Heidi Holman
Assistant General Counsel, Microsoft

Elizabeth Hyman
Chief Executive Officer, XR Association

Tatsuya Ichikawa
Chief Executive Officer, Avers

Stephanie Ifayemi
Global Shaper, London Hub

Rolf Illenberger
Managing Director, VRdirect

Michael Jacobides
Academic Adviser, BCH Henderson Institute, Boston Consulting Group (BCG)

Mikaela Jade
Founder and Chief Executive Officer, Indigital

Amy Jordan
Director, Technology Policy, Office of Communications (Ofcom)

Makarand Joshi
Director, Strategy, Innovation and Standards, Schneider Electric

Tony Justman
Vice-President and Deputy General Counsel, Sony Interactive Entertainment

Lea Kaspar
Executive Director, Global Partners Digital

Stephen Kavanagh
Executive Director, Police Services, International Criminal Police Organization (INTERPOL)

Masa Kawashima
Executive Producer, Director of Asia Pacific Operations, Niantic

Hoda Al Khzaimi
Assistant Research Professor, New York University, Abu Dhabi

Melissa Kiehl
Innovation & Foresight Advisor, ICRC

Ingrid Kopp
Co-Founder, Electric South

Ashish Kumar
Manager, Digital Strategy Office, Ministry of Communications and Information (MCI) of Singapore

Fabio La Franca
Founding Partner, Blueverse Ventures

Natalie Lacey
Executive Vice-President, Ipsos Media, Ipsos

Martina Larkin
Chief Executive Officer, Project Liberty

Su Kiang Lau
Executive Director, Conduct, SC Ventures, Financial Crime and Compliance, Standard Chartered

Sly Lee
Co-Chief Executive Officer and Co-Founder, Emerge

Helena Leurent
Director-General, Consumers International

Stephanie Llamas
Principal, Metaverse Foresight Strategy, VoxPop Insights

Dirk Lueth
Chairman, Open Metaverse Alliance for Web3 (OMA3)

Leon Lyu
Co-Founder, Booming Tech

Kuniyoshi Mabuchi
Managing Director, PwC Japan

Deena Magnall
Director, Global Digital and Technology Policy, L'Oréal

Noora Al Malek
Associate Project Manager, Artificial Intelligence Office, United Arab Emirates Government

Charles de Marcilly
Administrator, Council of the European Union

Eva Maydell
Member, European Parliament

Brett McDowell
Independent Chair, Hedera

Mauro Medico
Director, United Nations Counter-Terrorism Centre

Dinusha Mendis
Professor of Intellectual Property and Innovation Law, Bournemouth University

Jade Meskill
Vice-President, Product, Magic Leap

Anna Miyagi
Deputy Counsellor, Secretariat of Intellectual Property Strategy Headquarters, Cabinet Office of Japan

Hiroaki Miyata
Professor and Chair, Department of Health Policy Management, Keio University

Hamdullah Mohib
Managing Director, Khas Fund, Chimera Investment

Ahram Moon
Research Fellow, Centre for AI and Social Policy, Korea Information Society Development Institute

Steve Morris
International Chair, Portland Communications, Omnicom

Angelica Munson
Executive Officer, Chief Digital Officer, Shiseido

Eli Noam
Professor of Finance and Economics; Director, Columbia Institute for Tele-Information, Columbia Business School

Madan Oberoi
Executive Director, Technology and Innovation, INTERPOL

Genki Oda
Managing Executive Officer, SBI Holdings

Reinhard Oertli
Partner, Zurich, MLL Meyerlustenberger Lachenal Froriep

Judith Okonkwo
Founder, Imìsí 3D Creation Lab

Helen Papagiannis
Founder, XR Goes Pop

Charles Paré
Chief Integrity Officer, Head, Legal and Compliance, World Economic Forum

Park Yuhyun
Founder and Chief Executive Officer, DQ Institute

Erin Marie Parsons
Researcher, Escola Superior d'Administració i Direcció d'Empreses (ESADE)

Kavya Pearlman
Founder and Chief Executive Officer, XR Safety Initiative

Amy Peck
Founder and Chief Executive Officer, EndeavorXR

Bertrand Perez
Chief Executive Officer, Web 3.0 Technologies Foundation

Susan Persky
Director, Immersive Simulation Program; Head, Health Communication and Behavior Unit, National Institutes of Health

David Ryan Polgar
Founder and Executive Director, All Tech is Human

Nicola Port
Chief Legal Officer and Member of the Executive Committee, World Economic Forum

Saif Al Rahma
International Legal Advisory, Dubai Economic and Tourism Department, United Arab Emirates Government

Yonatan Raz-Fridman
Founder and Chief Executive Officer, Supersocial

Simmy Rease
Senior Legal Counsel/evision (e& life), e&

Michaël Reffay
Digital, Telecommunications and Postal Services, Permanent Representation of France to the European Union

Gina Reif Ilardi
General Counsel, Vindex

Dan Rice
Vice-President, Digital Governance, Walmart

Tim Roberts
Partner and Managing Director, UK Country Co-Leader, AlixPartners

Katitza Rodriguez
International Rights Director, Electronic Frontier Foundation (EFF)

Philip Rosedale
Co-Founder, High Fidelity

Sarah Sakha
Public Policy Manager, Meta Platforms

Erica Salinas
Principal Tech Leader, Web3, Amazon

Var Shankar
Director, Policy, Responsible Artificial Intelligence Institute

Nagwa El Shenawi
Undersecretary, Ministry of Communications and Information Technology of Egypt

Lewis Smithingham
Director, Creative Solutions, S4Capital

Ian Stevenson
Chief Executive Officer, Cyacomb

Philippe Stransky-Heilkron
Senior Vice-President and Chief Architect, Kudelski

Artur Sychov
Founder and Chief Executive Officer, Somnium Space

Claire Thwaites
Senior Director EMEA Government Affairs, The LEGO Group

Timmu Toke
Chief Executive Officer and Founder, Wolfprint 3D

Neil Trevett
President, Metaverse Standards Forum

Paul Trueman
Senior Vice-President, Cyber and Intelligence Solutions, Mastercard

Matthew Vick
Deputy Director, Futures and Innovation, HM Revenue and Customs

Steven Vosloo
Digital Policy Specialist, UNICEF

Larry Wade
Senior Director, Crypto/BC Risk and Compliance, PayPal

Kent Walker
President, Global Affairs and Chief Legal Officer, Google

Lynette Wallworth
Artist, Studio Wallworth

Alice Wang
Managing Director, Corporate and Investment Bank (CIB) Strategy, JP Morgan

Gregory Welch
Professor and AdventHealth Endowed Chair in Healthcare Simulation, University of Central Florida

Deborah Welsh
Executive Manager, International, Strategy and Futures Branch, eSafety Commissioner

Josh Williams
Chief Executive Officer, Forte

Jonathan Wong
Group President, Group ONE Holdings

Samer Yaghnam
Chief Legal and Administrative Officer, Olayan

Yu Yuan
President of IEEE Standards Association, Institute of Electrical and Electronics Engineers (IEEE)

Robby Yung
Chief Executive Officer, Animoca Brands

Erez Zaionce
Director, Centre for the Fourth Industrial Revolution Colombia

Production

Rose Chilvers
Designer, Studio Miko

Laurence Denmark
Creative Director, Studio Miko

Martha Howlett
Editor, Studio Miko

Endnotes

1. “Technology Vision 2024”, *Accenture*, 9 January 2024, https://www.accenture.com/us-en/insights/technology/technology-trends-2024.
2. “Digital Identity”, *PwC*, n.d., https://www.strategyand.pwc.com/de/en/industries/telecommunication-media-and-technology/digital-identity.html.
3. “What is the Metaverse?”, *Meta*, n.d., https://about.meta.com/what-is-the-metaverse/.
4. Metaverse Development Company, “The Real-World Metaverse: Bridging Physical and Digital Realities”, *Medium*, 27 July 2023, https://medium.com/@brewblocktechblockchain/the-real-world-metaverse-bridging-physical-and-digital-realities-e67ce99e8003.
5. Rene, Gabriel and Dan Mapes, *The Spatial Web*, Google Books, 2019.
6. “Home”, *Spatial Web Foundation*, https://spatialwebfoundation.org/.
7. Mapes, Dan, “An Introduction to The Spatial Web”, *Transformative Tech*, 16 August 2021, https://transformativetech.org/an-introduction-to-the-spatial-web/.
8. Rice, Tatiana, “When is Biometric no longer a biometric?”, *Future of Privacy Forum*, 19 May 2022, https://fpf.org/blog/when-is-a-biometric-no-longer-a-biometric/.
9. “Customize Your Meta Avatar With New Body Shapes, Hair and Clothing”, *Meta*, 27 April 2023, https://about.fb.com/news/2023/04/meta-avatars-new-body-shapes-hair-clothing/.
10. Ready Player Me, https://readyplayer.me/.
11. “Introducing ChatGPT”, *OpenAI*, n.d., https://openai.com/blog/chatgpt.
12. “Bard”, *Google*, https://gemini.google.com/.
13. “Azure Digital Twins”, *Microsoft*, https://azure.microsoft.com/en-us/products/digital-twins/.
14. Kamel Boulos, Maged N. and Peng Zhang, “Digital Twins: From Personalized Medicine to Precision Public Health”, *Journal of Personalized Medicine*, vol. 11, no. 8, 2021.
15. Nilga, Maria and Dmytro Rusin, “AR-based Indoor Navigation”, *Grid Dynamics*, 8 April 2021, https://blog.griddynamics.com/ar-based-indoor-navigation/.
16. “RASSAR”, *Makeability Lab*, n.d., https://makeabilitylab.cs.washington.edu/project/rassar/.
17. World Economic Forum, *Identity in a Digital World: A New Chapter in the Social Contract*, 2018, https://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf.
18. Ibid.
19. Accenture, *Human by Design* [video], https://videos.ces.tech/detail/video/6344580565112/human-by-design-presented-by-accenture.
20. Price, Matthew, “Part 1: From Human-Centric Design to Human-First Design in the Metaverse”, *Medium*, 3 April 2023, https://medium.com/@matthewpricephd/part-1-from-human-centric-design-to-human-first-design-in-the-metaverse-bad99598488a.
21. “Digital Trust”, *World Economic Forum*, n.d., https://initiatives.weforum.org/digital-trust/about.
22. “New report: Exploring human vulnerability in the metaverse”, *Alliance for Universal Digital Rights*, 17 July 2023, https://audri.org/new-report-exploring-human-vulnerability-in-the-metaverse/.
23. “Accenture Technology Vision 2024: “Human by Design” Technologies Will Reinvent Industries and Redefine Leaders by Supercharging Productivity and Creativity”, *Accenture*, 9 January 2024, https://newsroom.accenture.com/news/2024/accenture-technology-vision-2024-human-by-design-technologies-will-reinvent-industries-and-redefine-leaders-by-supercharging-productivity-and-creativity.
24. “The Metaverse: What It Is, Where to Find it, Who Will Build It, and Fortnite”, *The Ball Metaverse Index*, 13 January 2020, https://www.ballmetaverse.co/research/the-metaverse-what-it-is-where-to-find-it-who-will.
25. Pettifer, Stephen, Emma Barrett, James Marsh, Kathryn Hill, et al., *The Future of eXtended Reality Technologies, and Implications for Online Child Sexual Exploitation and Abuse*, 2022, https://documents.manchester.ac.uk/display.aspx?DocID=62042.
26. “Why ID matters for development”, *Identification for Development*, https://id4d.worldbank.org/guide/why-id-matters-development#:~:text=This%20global%20identification%20gap%20is,providing%20legal%20identity%20from%20birth.
27. “hegemony”, *Britannica*, https://www.britannica.com/topic/hegemony.
28. “anthropomorphism”, *Britannica*, https://www.britannica.com/topic/anthropomorphism.
29. Rufer-Bach, Kimberly, *The Second Life Grid*, Google Books, 2009, https://www.google.com/books/edition/The_Second_Life_Grid/IdSnTAHr45sC?hl=en.

30. “OECD Recommendation on the Governance of Digital Identity”, *Organisation for Economic Co-operation and Development*, 26 September 2023, https://www.oecd.org/digital/digital-government/oecd-recommendation-on-the-governance-of-digital-identity.htm.

31. UNICEF, *The Metaverse Extended Reality and Children*, 2023, https://www.unicef.org/globalinsight/media/3056/file/UNICEF-Innocenti-Rapid-Analysis-Metaverse-XR-and-children-2023.pdf.pdf.

32. World Economic Forum, *Privacy and Safety in the Metaverse*, 2023.

33. “The Child Safety Initiative”, *X Reality Safety Intelligence (XRSI)*, n.d., https://xrsi.org/programs/child-safety.

34. World Economic Forum, *Privacy and Safety in the Metaverse*, 2023.

35. Wu, Sixuan, Jiannan Li, Maurício Sousa and Tovi Grossman, *Investigating Guardian Awareness Techniques to Promote Safety in Virtual Reality*, Institute of Electrical and Electronics Engineers (IEEE), 2023, https://ieeexplore.ieee.org/document/10108418.

36. “Virtual assistant” *Wikipedia*, last edited 8 February 2024, https://en.wikipedia.org/wiki/Virtual_assistant.

37. Mayer-Schönberger, Viktor and Kenneth Cukier, *Big Data*, Google Books, 2013, https://www.google.com/books/edition/Big_Data/uy4lh-WEhhIC?hl=en.

38. Kröger, Jacob Leon, *Recognizing Information Inferred about Individuals as Personal Data*, Social Science Research Network (SSRN), 2022, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4349200.

39. Weingarden, Gary and Matthias Artzt, “Metaverse and privacy”, *International Association of Privacy Professionals (IAPP)*, 23 August 2022, https://iapp.org/news/a/metaverse-and-privacy-2/#:~:text=How%20does%20the%20metaverse%20affect,traced%20back%20to%20real%20individuals.

40. Taylor, Petroc, “Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2020, with forecasts from 2021 to 2025”, *Statista*, 16 November 2023, https://www.statista.com/statistics/871513/worldwide-data-created/.

41. Ibid.

42. Floridi, Luciano and Josh Cowls, “A Unified Framework of Five Principles for AI in Society”, *Harvard Business Review*, issue 1, no. 1, 1 July 2019, https://hdsr.mitpress.mit.edu/pub/l0jsh9d1/release/8.

43. Kröger, Jacob Leon, *Recognizing Information Inferred about Individuals as Personal Data*, SSRN, 2022, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4349200.

44. Faverio, Michelle, “How Americans feel about and manage data privacy: Key findings”, *Pew Research Center*, 18 October 2023, https://www.pewresearch.org/short-reads/2023/10/18/key-findings-about-americans-and-data-privacy/.

45. “Re-identification risk analysis”, *Google Cloud*, n.d., https://cloud.google.com/dlp/docs/concepts-risk-analysis#:~:text=Conversely%2C%20re%2Didentification%20is%20the,as%20medical%20or%20financial%20data.

46. Ibid.

47. Ibid.

48. Pariser, Eli, *The Filter Bubble: What the Internet is Hiding from You*, Penguin Press, 2011.

49. Whyman, Bill, “AI Regulation is Coming- What is the Likely Outcome?”, *Center for Strategic & International Studies (CSIS)*, 10 October 2022, https://www.csis.org/blogs/strategic-technologies-blog/ai-regulation-coming-what-likely-outcome.

50. European Parliament, *Artificial Intelligence Act: deal on comprehensive rules for trustworthy AI* (Press release), 9 December 2023, https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai.

51. “Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence”, *The White House*, 30 October 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/.

52. Miller, M.R., F. Herrera, H. Jun, J.A. Landay and J.N. Bailenson, “Personal identifiability of user tracking data during observation of 360-degree VR video”, *Scientific Reports,* vol. 10, no. 1, 2020.

53. Zuboff, Shoshana, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, Harvard Business School, 2019.

54. Carlini, Nicholas, Chang Liu, Úlfar Erlingsson, Jernej Kos et al., *The Secret Sharer: Evaluating and Testing Unintended Memorization in Neural Networks* in SEC’19: Proceedings of the 28th USENIX Conference on Security Symposium, 2019.

55. Ibid.

56. Porter, Alexis, “A Guide to Types of Sensitive Information”, *Big ID*, 5 May 2023, https://bigid.com/blog/sensitive-information-guide/.

57. Ibid.

58. Ibid.

59. Cieslik, Katarzyna and Dániel Margócsy, “Datafication, Power and Control in Development: A Historical Perspective on the Perils and Longevity of Data”, *Progress in Development Studies*, vol. 22, issue 4, 25 February 2022.

60. World Economic Forum, *Reimagining Digital ID*, 2023, https://www.weforum.org/reports/reimagining-digital-id/.

61. World Economic Forum, *Earning Digital Trust: Decision-Making for Trustworthy Technologies*, 2022, https://www.weforum.org/reports/earning-digital-trust-decision-making-for-trustworthy-technologies/.

62. INTERPOL, *INTERPOL launches first global police Metaverse* [Press release], 20 October 2022, https://www.interpol.int/News-and-Events/News/2022/INTERPOL-launches-first-global-police-Metaverse.

63. Cheong, B.C., "Avatars in the metaverse: potential legal issues and remedies", *International Cybersecurity Law Review*, issue 3, pp. 467-494, 2022, https://doi.org/10.1365/s43439-022-00056-9.

64. Schmitt, Paul et al., *The Decoupling Principle: A Practical Privacy Framework*, National Science Foundation, 2022.

65. World Economic Forum, *Advancing Digital Agency: The Power of Data Intermediaries*, 2022.

66. Kaye, Kate, "What data privacy could look like in the metaverse", *Protocol*, 16 February 2022, https://www.protocol.com/enterprise/data-privacy-intermediaries-metaverse-web3.

67. "eIDAS Regulation", *European Commission*, 17 May 2023, https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation.

68. "Trusted Digital Identity Framework (TDIF)", *Australian Government*, n.d., https://www.digitalidentity.gov.au/tdif.

69. "Trust Framework", *Digital ID & Authentication Council of Canada*, n.d., https://diacc.ca/trust-framework/.

70. "Digital Identity Services Trust Framework", *New Zealand Digital Government*, n.d., https://www.digital.govt.nz/digital-government/programmes-and-projects/digital-identity-programme/trust-framework/.

71. "UK digital identity and attributes trust framework", *GOV.UK*, 13 June 2022, https://www.gov.uk/government/publications/uk-digital-identity-and-attributes-trust-framework-beta-version.

72. "Digital Trust Centre (DTC)", *NTU Singapore*, https://www.ntu.edu.sg/dtc.

73. Vescent, Heather, "The Metaverse: A missed opportunity for data ownership and privacy?", *Biometric Update*, 21 January 2022, https://www.biometricupdate.com/202201/the-metaverse-a-missed-opportunity-for-data-ownership-and-privacy.

74. "Age Estimation", *Yoti*, n.d., https://www.yoti.com/business/facial-age-estimation/#:~:text=Facial%20Age%20Estimation%20is%20frictionless,accuracy%20%E2%80%93%20better%20than%20human%20judgement.

75. "Liquid Avatar Technologies", https://liquidavatartechnologies.com/.

76. Huntington, Gary, "Kids, Schools, AI/AR/VR, Legal Identities, Contracts and Privacy", *LinkedIn*, 16 July 2021, https://www.linkedin.com/pulse/kids-schools-aiarvr-legal-identities-contracts-guy-huntington/.

77. Wang, Siwen and Wei Wang, "A review of the application of digital identity in the Metaverse", *Security and Safety*, vol. 2, 2023, https://sands.edpsciences.org/articles/sands/pdf/2023/01/sands20220013.pdf.

78. "What is KYC?", *Swift*, n.d., https://www.swift.com/your-needs/financial-crime-cyber-security/know-your-customer-kyc/meaning-kyc.

79. Pivcevic, Katya, "User-centric digital ID, biometric KYC policy model proposed by financial inclusion group", *Biometric Update*, 5 October 2021, https://www.biometricupdate.com/202110/user-centric-digital-id-biometric-kyc-policy-model-proposed-by-financial-inclusion-group.

80. "Active Domain Groups", *Metaverse Standards Forum*, n.d., https://metaverse-standards.org/domain-groups/.

81. Broom, Douglas, "A billion people have no legal identity - but a new app plans to change that", *World Economic Forum*, 20 November 2020, https://www.weforum.org/agenda/2020/11/legal-identity-id-app-aid-tech/.

82. Sanders, Cynthia K. and Edward Scanlon, "The Digital Divide Is a Human Rights Issue: Advancing Social Inclusion Through Social Work Advocacy", *Journal of Human Rights and Social Work*, vol. 6, issue 2, pp. 130-143, 19 March 2021, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7973804/.

83. "Identification for Development Global Dataset", *World Bank*, n.d., https://id4d.worldbank.org/global-dataset.

84. "Digital footprint", *eSafety Commissioner*, https://www.esafety.gov.au/young-people/digital-footprint.

85. Lee, Jong-Eun Roselyn, "Does virtual diversity matter?: Effects of avatar-based diversity representation on willingness to express offline racial identity and avatar customization", *Computers in Human Behavior*, vol. 36, 2014, pp. 190-197, https://www.sciencedirect.com/science/article/abs/pii/S0747563214001629#:~:text=,2022%2C%20Journal%20of%20Computer.

86. Stets, J.E. and P.J. Burke, "Identity theory and social identity theory", *Social Psychology Quarterly*, vol. 63, no. 3, 2000, pp. 224-237.

87. Burke, P.J., "Relationships among multiple identities" in *Advances in Identity Theory and Research*, eds. P.J. Burke, T.J. Owens, R.T. Serpe, and P.A. Thoits, Springer, 2003, pp. 195-214.

88. Burke, P.J. and J.E Stets, *Identity Theory*, Oxford University Press, 2009.

89. Stets, J.E. and P.J. Burke, "Identity verification, control, and aggression in marriage", *Social Psychology Quarterly*, vol. 68, no. 2, 2005, pp. 160-178.

90. Sheth, Ronak, "Human-first vs. Digital first", *LinkedIn*, 5 January 2023, https://www.linkedin.com/pulse/human-first-vs-digital-first-ronak-sheth/.

91. Price, Matthew, "Part 1: From Human-Centric Design to Human-First Design in the Metaverse", *Medium*, 3 April 2023, https://medium.com/@matthewpricephd/part-1-from-human-centric-design-to-human-first-design-in-the-metaverse-bad99598488a.

92. McDowell, Maghan, “Shaping online avatars: Why our digital identities differ”, *Vogue Business*, 19 October 2021, https://www.voguebusiness.com/technology/shaping-online-avatars-why-our-digital-identities-differ.

93. “Filters on Snapchat: What’s Behind The Augmented Reality Curtain”, *Banuba*, 25 October 2021, https://www.banuba.com/blog/snapchat-filter-technology-whats-behind-the-curtain.

94. “Transcript for Mark Zuckerberg: First Interview in the Metaverse | Lex Fridman Podcast #398”, *Lex Fridman*, n.d., https://lexfridman.com/mark-zuckerberg-3-transcript.

95. “TikTok face filters rack up millions of views while stirring up controversy”, *ABCNews*, 28 February 2023, https://abcnews.go.com/GMA/Wellness/tiktok-face-filters-rack-millions-views-stirring-controversy/story?id=97443381.

96. “Depersonalization-derealization disorder”, *Mayo Clinic*, n.d., https://www.mayoclinic.org/diseases-conditions/depersonalization-derealization-disorder/symptoms-causes/syc-20352911#:~:text=Depersonalization%2Dderealization%20disorder%20occurs%20when,re%20living%20in%20a%20dream.

97. Peckmann, Carina, Kyra Kannen, Max C. Pensel, Silke Lux et al., “Virtual reality induces symptoms of depersonalization and derealization: A longitudinal randomised control trial”, *Computers in Human Behavior*, vol. 131, 2022, https://www.sciencedirect.com/science/article/pii/S0747563222000553.

98. “TikTok face filters rack up millions of views while stirring up controversy”, *ABCNews*, 28 February 2023, https://abcnews.go.com/GMA/Wellness/tiktok-face-filters-rack-millions-views-stirring-controversy/story?id=97443381.

99. Touchcast, *CNH Industrial brand New Holland collaborates with Microsoft and Touchcast at CES 2023 with a metaverse immersive experience* [Press release], 5 January 2023, https://touchcast.com/newsroom/cnh-industrial-brand-new-holland-collaborates-with-microsoft-and-touchcast-at-ces-2023-with-a-metaverse-immersive-experience.

100. “Emotionally Aware AI: ChatGPT Outshines Humans in Emotional Tests”, *Neuroscience News*, 13 May 2023, https://neurosciencenews.com/chatgpt-emotion-awareness-23231/#:~:text=,in%20diagnosing%20and%20treating%20psychopathology.

101. Ghosh, Shikhar, *Replika: Embodying AI*, Harvard Business School, 2023.

102. Hadero, Halehluya, “Amazon unveils a ‘smarter and more conversational’ Alexa amid AI race among tech companies”, *AP News*, 20 September 2023, https://apnews.com/article/amazon-alexa-generative-ai-updgrade-0d02285b169fa24faf3ecbf259b31d82.

103. Li, Xinge and Yongjung Sung, “Anthropomorphism brings us closer: The mediating role of psychological distance in User–AI assistant interactions”, *Computers in Human Behavior*, vol. 118, 2021, https://www.sciencedirect.com/science/article/abs/pii/S0747563221000029#:~:text=One%20of%20the%20most%20frequently,864.

104. Tang, Liang and Masooda Bashir, “Do We Trust Embodied Agents who Look Like us?”, *IEEE*, 2023, https://ieeexplore.ieee.org/document/10294444.

105. “Miquela Sousa”, *Virtual Humans*, n.d., https://www.virtualhumans.org/human/miquela-sousa.

106. Nair, Vivek, Gonzalo Munilla Garrido and Dawn Song, “MetaGuard: Going Incognito in the Metaverse” in *Proceedings of the 36th Annual ACM Symposium on User Interface Software and Technology (UIST ‘23)*, Berkley RDI, 2023, https://doi.org/10.1145/3586183.3606754.

107. Gao, Qiaozi (QZ), Govind Thattai, Suhaila Shakiah, Xiaofeng Gao et al., *Alexa Arena: A user-centric interactive platform for embodied AI*, Amazon Science, 2023, https://www.amazon.science/publications/alexa-arena-a-user-centric-interactive-platform-for-embodied-ai.

108. Mitrushchenkova, A.N., “Personal Identity in the Metaverse: Challenges and Risks”, *Kutafin Law Review*, vol. 9, no. 4, 2022, https://kulawr.msal.ru/jour/article/view/190.

109. Schulmeyer, Julia, *Guardians of the Metaverse: Expert Assessment of Emerging Privacy Challenges and Mitigation Strategies*, Association for Information Systems, 2023.

110. Ullrich, Daniel, Andreas Butz and Sarah Diefenbach, “The Development of Overtrust: An Empirical Simulation and Psychological Analysis in the Context of Human–Robot Interaction”, *Frontiers*, 2021, https://www.frontiersin.org/articles/10.3389/frobt.2021.554578/full.

111. Bontridder, Noémi and Yves Poullet, “The role of artificial intelligence in disinformation”, *Cambridge University Press*, 25 November 2021, https://www.cambridge.org/core/journals/data-and-policy/article/role-of-artificial-intelligence-in-disinformation/7C4BF6CA35184F149143DE968FC4C3B6.

112. Rosenberg, Louis, “The danger of AI micro-targeting in the metaverse”, *VentureBeat*, 27 January 2022, https://venturebeat.com/ai/the-danger-of-ai-micro-targeting-in-the-metaverse/#:~:text=And%20because%20these%20AI%20agents,we%20need%20to%20regulate%20some.

113. Zimmermann, Daniel, Anna Wehler and Kai Kaspar, “Self-representation through avatars in digital environments”, *Current Psychology*, vol. 42, 2023, pp. 21775-21789, https://link.springer.com/article/10.1007/s12144-022-03232-6.

114. Signé, Landry, “Fixing the global digital divide and digital access gap”, *Brookings*, 5 July 2023, https://www.brookings.edu/articles/fixing-the-global-digital-divide-and-digital-access-gap/.

115. Abat, Manuel, “The Role Of AI In Building A Responsible Metaverse”, *Oliver Wyman*, October 2022, https://www.oliverwyman.com/our-expertise/insights/2022/oct/the-role-of-ai-in-building-responsible-metaverse.html.

116. “AI Ethics & Governance”, *Accenture*, n.d., https://www.accenture.com/us-en/services/applied-intelligence/ai-ethics-governance.

117. "Principles and approach", *Microsoft AI*, n.d., https://www.microsoft.com/en-us/ai/principles-and-approach.

118. "Responsible AI", *Meta*, n.d., https://ai.meta.com/responsible-ai/.

119. "wastonx.governance", *IBM*, n.d., https://www.ibm.com/products/watsonx-governance?utm_content=SRCWW&p1=Search&p4=43700078376398933&p5=b&gclid=EAIaIQobChMI5OKnhNnVgwMVZB6tBh3nwwjqEAAYASAAEgJS5fD_BwE&gclsrc=aw.ds.

120. "Our Workstreams", *World Economic Forum AI Governance Alliance*, n.d., https://initiatives.weforum.org/ai-governance-alliance/workstreams.

121. "Human-centered Artificial Intelligence", *Stanford University*, n.d., https://hai.stanford.edu/.

122. King, Jen, "Guide to influencer marketing: trends, tactics, and KPIs", *Insider Intelligence*, 26 January 2024, https://www.insiderintelligence.com/insights/influencer-marketing-report/#:~:text=The%20influencer%20marketing%20industry%20is,gold%20standard%20for%20the%20group.

123. Ong, Thuy, "Virtual Influencers Make Real Money While Covid Locks Down Human Stars", *Bloomberg*, 29 October 2020, https://www.bloomberg.com/news/features/2020-10-29/lil-miquela-lol-s-seraphine-virtual-influencers-make-more-real-money-than-ever?leadSource=uverify%20wall.

124. League of Legends, "K/DA - POP/STARS (ft. Madison Beer, (G)I-DLE, Jaira Burns) | Music Video – League of Legends", *YouTube*, 3 November 2018, https://www.youtube.com/watch?v=UOxkGD8qRB4.

125. Kaur, Harmeet, "Capitol Records drops 'robot rapper' FN Meka over criticism that the virtual character was offensive to Black artists", *CNN*, 24 August 2022, https://edition.cnn.com/2022/08/24/entertainment/fn-meka-dropped-capitol-records-cec/index.html.

126. World Economic Forum, *Privacy and Safety in the Metaverse*, 2023.

127. Mishler, Kary, "Who Is Responsible For Helping To Keep The Metaverse Safe?", *Robots.net*, 19 September 2023, https://robots.net/ai/who-is-responsible-for-helping-to-keep-the-metaverse-safe/#:~:text=Developers%20and%20platform%20operators%20play%20a%20critical%20role,software%2C%20and%20systems%20that%20power%20the%20virtual%20experience.

128. Shweta, Kelly Main and Keatron Evans, "What Is Smishing? Definition, Examples & Protection", *Forbes Advisor*, 1 August 2023, https://www.forbes.com/advisor/business/what-is-smishing/.

129. Saha, Bidisha, "China Uses AI Deepfake avatars as 'news anchors' to spread disinformation", *India Today*, 8 February 2023, https://www.indiatoday.in/world/story/china-uses-ai-deepfake-avatars-as-news-anchors-to-spread-disinformation-2332165-2023-02-08.

130. Yang, Zeyi, "The deepfake avatars who want to sell you everything", *MIT Technology Review*, 20 September 2023, https://www.technologyreview.com/2023/09/20/1079885/chinese-deepfake-livestream-foreign-language/.

131. Helmus, Todd C., *Artificial Intelligence, Deepfakes, and Disinformation: A Primer*, RAND, 2022, https://www.rand.org/pubs/perspectives/PEA1043-1.html.

132. McDougald, Damon, "Digital Identity: The What, Why and How", *Accenture*, 19 April 2021, https://www.accenture.com/us-en/blogs/security/digital-identity-what-why-how.

133. UNICEF, *The Metaverse, Extended Reality and Children*, 2023.

WORLD ECONOMIC FORUM

COMMITTED TO
IMPROVING THE STATE
OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org