International Journal of Web Based Communities

ISSN online: 1741-8216 - ISSN print: 1477-8394
https://www.inderscience.com/ijwbc

Beyond avatars and access: rethinking digital identity governance in the metaverse

Nishant Anand, Bidyut Hazarika

DOI: 10.1504/IJWBC.2026.10079854

Article History:

Received:	15 July 2025
Last revised:	06 May 2026
Accepted:	20 May 2026
Published online:	21 July 2026

Beyond avatars and access: rethinking digital identity governance in the metaverse

Nishant Anand

Department of Science, Technology, Engineering and Public Policy,
University College London,
London WC1E 6JA, UK
Email: Nishant.anand.19@alumni.ucl.ac.uk

Bidyut Hazarika*

Department of Business Information Systems,
Haworth College of Business,
Western Michigan University,
1903 W Michigan Ave.,
Kalamazoo, MI 49008-5412, USA
Email: bidyut.hazarika@wmich.edu
and
Department of Innovation,
The Business School,
RMIT Vietnam,
702 Nguyen Van Linh Blvd., District 7,
Ho Chi Minh City, Vietnam
Email: bidyut.hazarika@rmit.edu.vn
*Corresponding author

Abstract: Digital identity in the metaverse extends beyond authentication to include avatars, personas, credentialing systems, IoT-mediated traces, and relational data generated through immersive interaction. This paper develops a framework for analysing these identity dimensions and applies it to three workshop-based scenarios: social media influencing, corporate XR work, and public-private healthcare. The findings show that immersive environments blur boundaries between public and private life, intensify datafication, and shift power and value toward platforms, employers, and infrastructure providers. These dynamics expose the limits of governance models based mainly on consent, transparency, and fixed distinctions between personal and sensitive data. Because responsibility is distributed across multiple actors, accountability becomes difficult to assign, while existing regulatory tools struggle to address harms to autonomy, privacy, dignity, and identity formation. The paper argues for rights-centred, socio-technical governance based on value-sensitive design, human rights impact assessments, transnational coordination, and stronger user participation and oversight.

Keywords: metaverse; digital identity; eID; governance; human rights.

Reference to this paper should be made as follows: Anand, N. and Hazarika, B. (2026) 'Beyond avatars and access: rethinking digital identity governance in the metaverse', *Int. J. Web-Based Communities*, Vol. 22, No. 5, pp.1–32.

Biographical notes: Nishant Anand received his PhD in Digital ID Governance: A Critical Research Agenda from the Department of Science, Technology, Engineering and Public Policy (STEaPP) at University College London. His research interests are in the governance and impacts of emerging technologies. The motivation of this research is to critically analyse emerging technologies, in particular digital systems, and bring to bear their socially constructed nature. While acknowledging the potential of these systems, his research aims to address issues of dataism and provide solutions to bridge the digital divide.

Bidyut Hazarika is an Associate Professor in the Department of Business Information Systems at Western Michigan University and a Senior Lecturer in the Business Innovation Department at RMIT Vietnam. He holds a PhD in Computer Science and Information Systems from the University of Colorado Denver and an MBA in Information Systems and Finance from the University of Toledo. His research focuses on digital business, information systems, consumer technology adoption, mobile applications, cross-border e-commerce, social media, and emerging technologies. His work has been published in journals such as *Acta Psychologica*, *Computers in Human Behavior*, *Journal of Global Information Management, Industrial Management & Data Systems*, and *Global Knowledge, Memory and Communication*. He has also taught and developed courses in artificial intelligence in business, business analytics, cybersecurity, user experience design, and cross-border e-commerce.

1 Introduction

The metaverse is speculated to be the future of the internet, a new digital frontier for individuals, business, and governments to participate in. Its naming, derived from science fiction literature, aims to evoke a digital imaginary that is completely immersive for its users – raising new possibilities for social and economic connections and generating concerns over user safety, privacy and personal autonomy. Its value proposition stems from the promise of spatial interactions (not limited to 2D screens), persistence of identity and scenery, interoperability (across metaverse ecosystems), and the blending of physical and virtual worlds using interconnected technologies such as digital twins, augmented reality (AR) headsets, sensors and real time spatial computing. Industry experts speculate that the metaverse market is expected to be worth $800 billion by 2025 and generate over $1 trillion in GDP through its deployment in numerous use cases spanning education, advertising, government, and entertainment sectors (Bloomberg, 2021; Deloitte, 2022; Hadi et al., 2023). The metaverse offers an important framing as well. It provides an anchor point for imagining the impacts of frontier technologies and immersive digital ecosystems, highlighting where future innovations may occur as the risks and harms within these environments.

This paper especially focuses on digital identity in the metaverse. Digital identity is not only an entry point for accessing the metaverse but also includes avatars created in the environment, and the multitude of interactions users may have within it. This study builds a novel framework for understanding digital identity in the metaverse that considers the technical, social, spatial and temporal aspects associated with identity formation in dynamically rendered environments. Using case studies and participatory workshops this paper showcases how current governance instruments, used to balance

risks and opportunities in digital environments, are inadequate for immersive environments like the metaverse. The locus of evaluation on digital identity is important as it the core area where economic imperatives within the metaverse clash against human rights objectives. Thus, managing these often-divergent interests becomes an important avenue for governance studies. Currently, there is limited academic research that has critically evaluated metaverse governance, this study offers a first such investigation in this space.

An additional novelty of this study is in the methodology. Empirical data collection was done with young adults on metaverse scenarios. This study helps to understand how young adults, as digital natives, perceive their identities, metaverse systems and the potentialities associated with them. In this study, three specific research questions are investigated within the context of the metaverse:

- What is the role of digital identity (eID) in the metaverse?
- What risks to eIDs exist in the metaverse?
- What initiatives do system stakeholders need to consider in governing eIDs responsibly?

By using specific scenarios, this study highlights how current regulation, built around concepts of personal and sensitive data, may be ineffective in such environments and how users are limited in their locus of control over their identity when faced by the deployment of metaverse like systems. Not addressing the risks can lead to distrust in the system and subsequent lack of adoption. This study proposes a re-evaluation of existing governance approaches, emphasising a need for rights-based regulatory and governance interventions to address the risks of invasive technologies and immersive digital ecosystems.

The paper is organised as follows. It first presents an overview of the literature pertaining to metaverse. Next, the research method, data collection, and results are then presented. The paper concludes with a discussion of the research results, limitations and suggestions for future research.

2 Literature review

2.1 The metaverse

Descriptions of the metaverse, both in literature and in its up-and-coming deployments, anchor around the idea of ‘immersiveness’. This suggests an ability to actively engage a user’s senses and thereby alter their mental state to feel as if they are within the metaverse. This description requires deconstructing, both from a user experience perspective as well as from a transformational narrative perspective.

For users to feel fully immersed, four features are necessary: realism, ubiquity, interoperability, and scalability (Dionisio et al., 2013). Realism points to creating ‘digital reality’ – a spatial and temporal environment which enables users to engage with the environment at a psychological and emotional level, thus requiring engagement with multiple human senses. Not only will a user need to see in three dimensions, be able to make and respond to facial gestures but also be able to hear in surround sound, feel touch and possibly taste or smell in the metaverse. Ubiquity relates to two distinct

sub-concepts: ubiquitous availability of the metaverse and ubiquitous availability of identity. An individual's experience of the physical world is that it persists with or without the individual in it. Ubiquitous availability of the metaverse suggests that digital sociality should continue regardless of whether a user is immersed in it. Ubiquity of identity pertains to mimicking an individual's lived experience, where they can navigate space and time with a persistent identity. This identity can be displayed through physical features, institutionally assigned documentation, or even through habits, behaviours, and interactions with its environment. Metaverses require a similar conception of identity – ubiquitously available across metaverse spaces. Interoperability is the ability to allow disparate virtual worlds to seamlessly interact with one another and enable artefacts of one virtual world to persist in another virtual world (Dionisio et al., 2013). Only through this compatibility across virtual worlds can the metaverse develop into a successor to the internet and mimic an individual's experience of navigating reality seamlessly. This points not just to technical interoperability but also the requirement for commercial agreements and standard contracts to operationalise the experience across metaverse service providers. Finally, scalability is the ability for the metaverse to create and expand without service degradation. Scalability considerations are threefold (Dionisio et al., 2013; Liu et al., 2010): scalable environments in the face of concurrent users, scene complexity and dynamic interactions between users and their environments. Achieving the four tenets in the metaverse requires crucial decisions on architectural choice, technology selection, as well as commercial partnership arrangements.

From a narrative standpoint, the metaverse suggests a digital leap beyond the current experience of the internet, through a 2-dimensional screen, and into a cyber-physical world where the user is interacting and creating data dynamically. It is an important narrative that helps direct investment and engagement into the idea and its supporting technologies, as a transformational next step in the evolution of the internet and our interactions with digital mediums.

2.2 Digital identity in the metaverse

Digital identity in the metaverse, it is not just about identification as an entry process but also includes the personas and avatars created in the metaverse, and the multitude of interactions users may have within the dynamic environment. Identities – physical or digital – are impacted by the possibilities and constraints of the surrounding environment. In the metaverse, dynamically rendered environments provide a unique set of possibilities for an individual to explore. It also creates a gateway for continuous and exponential data extraction, analysis, and monetisation. Digital identity, within the metaverse, thus becomes an arena for continuous value creation or exploitation. This section provides an overview of the different digital identity attributes that are created in the metaverse. Figure 1 provides a summative framework of the aspects of digital identity relevant in the metaverse.

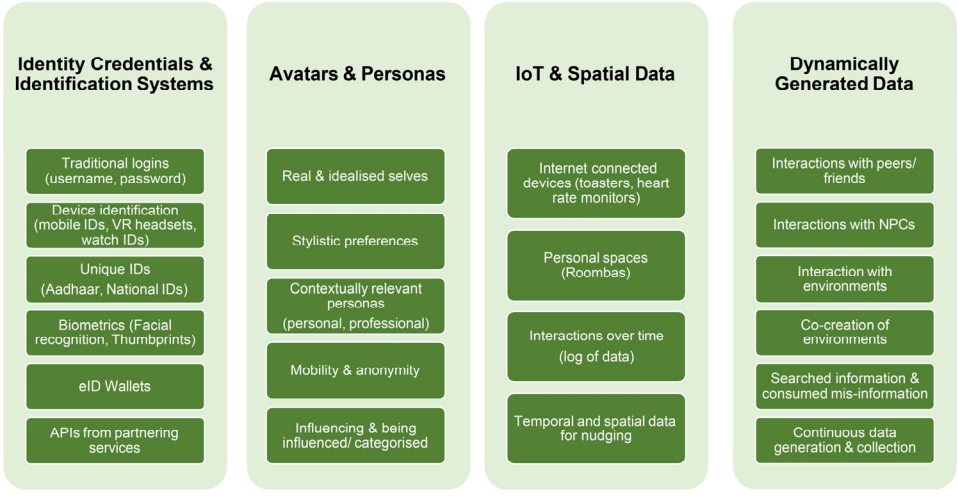
2.2.1 Identity credentials and identification systems

Accessing a metaverse will require identification credentials, not dissimilar to login credentials of today. Given the expansiveness of the metaverse, identification could be done via multiple methods:

- traditional logins (username, password)
- device identification (mobile phone IDs, XR headsets, watch IDs, IoT devices)
- unique IDs (Aadhaar, national IDs)
- biometrics (facial recognition, thumbprints, iris scans)
- eID wallets
- APIs from partnering services

While different metaverses may use different combinations of the above, greater accessibility requires multiple entry points. This creates interesting challenges for service providers. Exclusions may occur if enough entry points are not provided or if certain technologies are given priority over others. For example, mandatory service specific logins (like usernames and passwords) may exclude groups that are not digitally savvy or mandatory use of specific ID solutions, such as biometrics, may exclude groups that have historically been targeted or discriminated against using said technologies. Facial recognition is notoriously inaccurate when applied to people of colour, iris scans are suboptimal solutions for cataract patients, fingerprint scans less accurate for manual labourers have significantly higher failure rates in biometric registration due to fading thumb imprints (Rao, 2018; Sobti et al., 2020; Williams, 2020). On the other hand, multiple entry points create infrastructures of surveillance as well as security risks. Connectivity across devices and services enables corporations to buy and sell data and build 360-degree profiles of individuals. This allows for mass surveillance at low cost (Clarke, 2019). This practice can happen without the individual's knowledge and in large enough datasets can even be done where personally identifying information, such as name and age, are absent (Bradbury, 2021).

Figure 1 A framework for digital identity in the metaverse (see online version for colours)



Identity credentials create the building blocks for the bureaucratisation of data collection and analysis. It standardises identity in digital systems, which in the physical world is a

transient experience. This standardisation lays the foundations for future data collection, analysis, and exploitation (Hu, 2017). Being able to consolidate unique identifiers – digital, biometric, device related – allows organisations to analyse data in ways that may infringe on privacy and autonomy. Data loss due to lax security practices disproportionality affects the individuals and can lead to financial loss and identity fraud, with limited avenues for recourse. In centralised architectures, the risks are compounded where a single breach can expose the vulnerability in the entire architecture (Jain, 2023).

Sullivan (2016) categorises the above listed identification parameters as transactional identity attributes as they form a key piece in any subsequent transaction done post identification. Transactional identity enables a machine-to-machine transaction, where the human is no longer central to its occurrence (Sullivan, 2016). Here Sullivan highlights that system errors or malfunctions may lead to a transaction occurring against a transactional ID, which implicates a human regardless of their presence.

2.2.3 Avatars and personas

Metaverses provide the ability to create digital twins or 'avatars'. An avatar, per Hindu mythology, is an incarnation of a God usually in human form to embody a concept or philosophy that the story tries to convey. The supernatural being may have multiple avatars, each one symbolising a specific trait needed for the context. Digital platforms borrow the idea of avatars as means for its users to create their digital personas. An avatar could be a simple 2D animation, where the user can select attributes like skin colour, hair colour, and stylistic considerations such as clothes and eyewear. More complex avatars include full body representations that also respond to body movements of the user, interacting with the environment in a more realistic way.

Avatars can be fun representations of an individual but also represent personal identity information. It could be as simple as the general human features of the user (skin colour, eye colour, hair colour) or provide an insight into aspirational ideals of the individual. Avatars can represent aesthetics or even sexualities that a user may want to explore digitally, while feeling incapable of doing so in the offline world. Through their representations avatars may provide users greater social mobility, by obscuring offline identities and freedom from stigma, or immobility by exposing users to cyber-bullying, judgement, and harassment in digital environments (Davis and Chansiri, 2019).

In 'The Presentation of Self in Everyday Life', Goffman (1959) highlights how identity formation is a process of interaction between the performer (the individual), their environment (the metaverse), and the audience (other users, AI characters) they are performing to. The interaction between the performer, the environment and the audience legitimises the identity created. Goffman's conceptual model can be applied to avatars created in the metaverse. In corporate settings, an individual may want their avatar to project professionalism through a choice of attire and background setting, while in social metaverses the same individual may choose avatars to look and behave differently. Users may want to keep distinct identities in different settings, however, may not always be in control of this phenomenon. Offline friends may break the online image created by an individual by sharing intimate pictures or videos, corporate colleagues may stumble on personal avatars of individuals or data may inadvertently be shared across platforms by users themselves, just by using the same login processes (Moncur et al., 2016). These events may break the persona image that the individual wants to create within each environment.

There is a growing body of literature on online harms, harassment and identity fraud pertaining to avatars in virtual worlds. Harassment often is targeted at minorities, in particular women, LGBTQ+ communities and ethnic minorities. Harassment can range from verbal abuse to groping and rape in the metaverse (Freeman et al., 2022; Schulenberg et al., 2023). In the metaverse, the victim is not just affected with textual content, but also with words they hear and with physical actions such as groping that create haptic feedback. Co-mingling of age groups, anonymised via avatars, may also mean children are exposed to similar verbal and physical harassment. Anonymous avatars used by harassers may leave victims with limited options for recourse. While platform tools may exist, such as reporting and blocking users, they tend to be reactionary capabilities after an incident has occurred (Schulenberg et al., 2023).

Human identity is complex, multi-layered, and dynamic – it is constantly changing as an individual travels through time, space, and interacts with society and culture. Complex human identities, when flattened into code and resurfaced as avatars, create simplified versions of human identity. The simplicity may come at a heightened cost of surveillance, categorisation, and discrimination. Avatars with specific characteristics may be targeted for commercial gain or national interest purposes. Hegemonic categorisations may create limitations for individuals who may be trying to change their identities and social contexts (Schoemaker et al., 2021).

AI-powered avatars may represent individuals in the metaverse, without the individual having logged in. Bumble CEO, Whitney Wolfe, highlighted how AI-powered avatars could act as dating concierges in the future and transact with other avatars before zeroing down on a shortlist for a person to meet in real life (Tolentino, 2024). LinkedIn co-founder, Reid Hoffman, interviewed a hyper-realistic AI-powered Avatar of himself that had been trained on Mr Hoffman‟s published content to show the extendibility of human experience through digital technologies (Paul, 2024). In each of the contexts, avatars are implicating individuals even when the individual is absent. This creates a significant avenue of risk, identity fraud if the AI-avatars are compromised and may implicate individuals of crimes done by their avatars without their knowledge (Sullivan, 2016).

2.2.4 IoT, spatial and temporal data

Physical objects are increasingly being embedded with sensors and software that allow them to be connected to the internet. In home settings, these so called ‘smart devices’ can range from toasters to heart rate monitors and often come with apps that allow a user to interact with the device remotely. These devices rely heavily on internet connectivity and remote computing to perform their functions. However, they also have poor security controls and can be relatively easy to compromise, thus creating networked risks within the sociotechnical infrastructure that they are a part of, be that corporations, the internet, or a metaverse (Brass and Sowell, 2021). Cyber risks caused through IoT vulnerabilities can have impacts on an individual’s physical lives. In 2020, iRobot’s Roomba recorded a woman on the toilet then sending the images to a contracting company for labelling and training AI. Approximately 2 million images of homes were sent to this contractor by iRobot, whose defence was that users have consented to this service as part of a special agreement on select devices. The images, however, also ended up on numerous Facebook groups (Guo, 2022).

Connecting IoT devices to the metaverse can provide individuals with a means of extending their identity into the cyberspace. For example, the log from a smart watch can be a competitive boost between friends in a metaverse social circle. However, insufficient privacy measures may permit for-profit entities to access, aggregate, and utilise this data without the user's knowledge.

Human identities are constantly evolving with time and through the spaces they interact with. Physical or digital spaces create constraints or opportunities for identity realisation and experimentation to be done privately. With time identities evolve, preferences change, habits die or develop, and interactions with the world around changes. IoT-enabled technologies can create a persistent data-log of an individual's interactions in space and time. This data can then be organised and categorised for economic exploitation and value creation while creating significant vulnerabilities for the individuals and limiting their ability for safe and intimate identity exploration. Allotted categories may themselves be based on stereotypical tropes associated with age, gender or race that cause discrimination and may be hard to shake off once marked against.

2.2.5 Personal data in dynamically generated environments

The metaverse offers a wide variety of experiences be it concerts, museum tours or learning experiences. While engaging with these experiences, personal data is constantly created. This data can be on a spectrum of simple transactional logs such as logins/logout times or sensitive data explicating personal preferences. As individuals interact with these experiences the boundaries of who owns this data can be increasingly hard to tell. An example could be an artist – like Steve Aoki – performing at a Metaverse concert. Attendees to the concert are given POAP – proof of attendance protocol – that allows entrance and becomes a digital asset and allows the event hosts and sponsors to remain in contact with the attending fan (RLTY, 2022a, 2022b). In the concert, the fan may browse and purchase memorabilia, which is delivered to them as physical or digital goods. The fan may interact with concert goers and AI generated concert helpers. The concert may turn out to not be of the fans liking and they may leave early. The movements, interactions, purchases of the fan may all seem mundane but when done in a dynamic digital environment means that these mundane traces can be recorded and analysed. In the physical world this event represents an individual navigating through space and time, without always being tracked. Yet in the metaverse, the environment is not free from surveillance, and every mundane action can be tracked, recorded and analysed.

Strictly speaking not all the above-mentioned interactions relate to definitions of personal or sensitive data. Yet in the age of big data analytics the demarcations of personal and non-personal data or sensitive and non-sensitive data may be ineffective. With large enough datasets non-sensitive data can provide inferences about sensitive data (Solove, 2024). In fact, Sweeney (2000) demonstrated that 87% of people were identifiable in a dataset, based on just three attributes: post code, birth date, gender). In the above example, the fans purchase log, interactions with AI-bots could provide derivations on age, demographics, preferences and possible associations. This, over time, using POAPs can be used to continue to profile, recommend and nudge users into more interactions, purchases, and thereby more revelation of personal data. Per GDPR, personal and sensitive data categories require a lawful basis for collection and processing (GDPR, 2016). While there are six lawful bases for data processing, consent plays a substantial role. Given the mundane nature of the metaverse concert example above,

individual transactions may not surmount to personal data collection and thus not require consent from the outset but over time the data volume and associations can lead to revelations on personal and sensitive data. This poses a unique problem for regulation that is built around delineations of personal vs. non-personal data or sensitive vs. non-sensitive data. Similar gaps exist in privacy regulation globally, as they tend to be based around similar logics of attribution towards personal and sensitive data (Greenleaf, 2019; Solove, 2024). These gaps become ever more severe in dynamic environments such as the metaverse, where data is constantly and exponentially generated as individuals navigate through its environment.

To tackle the increased rates of mental health issues, the metaverse provides an opportunity to roll out virtual environments for therapists to engage with patients that may prefer virtual environments and the pseudo-anonymity of avatars to engage in therapy (Cerasa et al., 2022). Virgils, a VR startup for youth therapy, provides one such example. The novel environment may help engage with patients in environments they are more comfortable in and provide a conduit to exposure therapy to help face one's anxieties. AI-powered, virtual agents may assist in guiding patients through therapeutic experiences and extend medical professional reach. In contrast to a concert, a vast portion of all the interactions in this scenario may be associated with personal and sensitive data. Not just the content of discussion between the patient and therapist but also the login to therapy services, environments and avatars selected, as well as any engagement with AI-agents. It becomes a contested area of discussion around who owns, has access to, and processes this data. Given the networked nature of technological environments, this data may be shared across various health and non-health providers. Even seemingly impersonal information – such as date and time stamps for logging in to a therapy session – may over time provide information, which when associated with other attributes can lead to the development of profiles for targeting. The interactions between the therapist and the patient may be used in the development and training of AI-agents as well.

Dynamically generated, immersive environments may provide imagination-extending experiences but come at a cost of continuous surveillance, data collection and processing. It showcases how privacy law, steeped in data classifications, are inadequate to protect users. The interactions with the environment and AI-agents make it complicated to provide informed consent and resigns a user to by tracked continuously. As Solove (2024) opines a different method for privacy protection is needed; one that is based on an assessment of harm and risk within digital environments and not based on untenable data classifications. The metaverse may be a crucial use case in that matter.

3 Research methodology

The research methodology used for this study followed two distinct steps:

a building a common baseline for eID in the metaverse as described in Section 2

b engagement with end-users of metaverse technologies through cases studies (scenarios) that highlight the complexity of eID manifestations in different scenarios.

The literature review provides a baseline understanding of the metaverse and its key concepts. This was done by querying academic databases, such as SCOPUS and Web of Science, technical databases such as IEEE Explore, and grey literature found through

ResearchGate and Google Scholar. The literature review found gaps in academic publications around digital identity in the metaverse and hence was supplemented with grey literature and private sector research. This provided a foundation through which the fieldwork scenarios were created. The three scenarios cover the following areas:

- scenario 1: influencers in the metaverse
- scenario 2: working in the corporate metaverse
- scenario 3: seeking healthcare in a public-private metaverse.

The case studies served as input to workshops conducted with University College London (UCL) Master of Public Administration (MPA) students. Students were asked to consider the following research questions from the standpoint of each use case.

- What is the role of digital identity (eID) in the metaverse?
- What risks to eIDs exist in the metaverse?
- What initiatives do system stakeholders need to consider in governing eIDs responsibly?

Figure 2 Age distribution (see online version for colours)

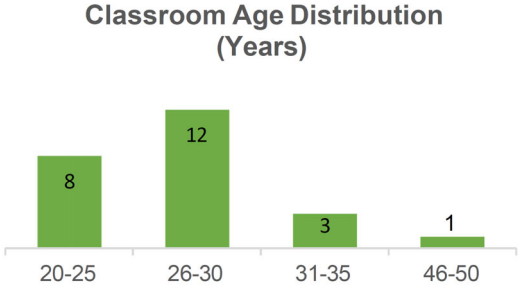
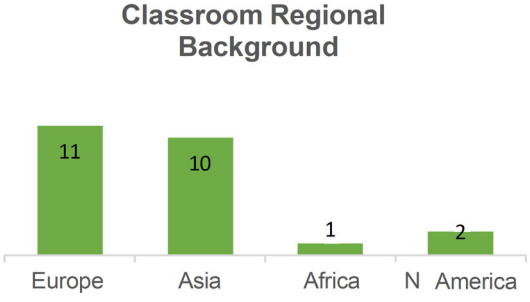


Figure 3 Regional background (see online version for colours)



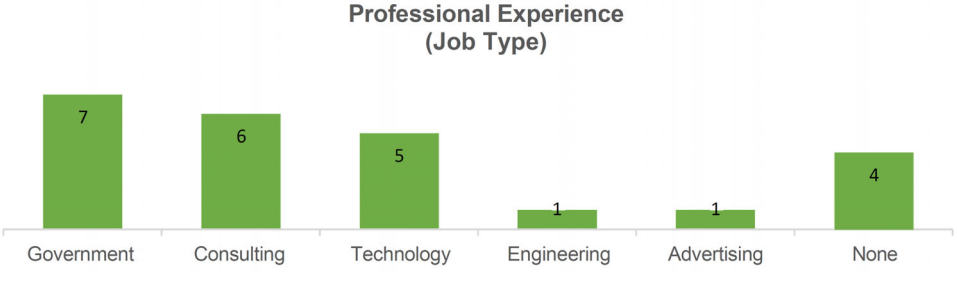
The choice of MPA students as workshop participants was a conscious one, as it allows a younger, digital native generation to engage with complex questions about eID governance in immersive digital environments. They are both in the know about immersive technologies (through gaming and concerts) and hold a normalised belief that digital tracking and surveillance are a 'reality' that is hard to challenge. Prior to case study analysis, students were surveyed on their awareness of foundational concepts of

digital identity and the metaverse. Survey results are summarised in Figures 2–5 and Table 1.

- Digital identity awareness: 85% understood eID data includes multiple identifiers, and 96% recognised its cross-sector applications.
- Control and risks: 87% lacked confidence in managing their eID data, questioning consent mechanisms. 68% agreed identity data holds economic value but debated who benefits. Concerns included privacy erosion and inequitable risk-reward trade-offs.
- Metaverse understanding: 79% saw it as a broad term or corporate marketing tool, with familiarity from gaming and entertainment.

Figure 4 Years of professional experience (see online version for colours)

Figure 5 Type of professional experience (see online version for colours)



For the case study analysis, students were divided into three groups. Each group had a note taker: one professor, one associate professor, one PhD student along with the facilitator (primary author). Each of the note takers were embedded in a case scenario and were provided with a set of questions to help guide the discussions. The questions were aimed at supporting discourse around eID risks, opportunities and governance interventions. Prior to the lecture the note takers and facilitator met to discuss a standard way for running each scenario and capturing notes. Note taking would cover the discussion within the group. The notes taken were descriptive of the discussion following the questions posed to them.

Table 1 Classroom Kahoot survey responses (see online version for colours)

Q	*Detail*	*Options*						*Total*
1	Which of the following are part of your digital identity? (multiple answers allowed)	*Login credentials (usernames, passwords, biometrics)*	*Personal data created about you (credit history)*	*Personal data created by you (pictures, tweets) and for you (IoT devices)*	*All of the above*			26
		3 12%	1 4%	0 0%	22 85%			
		TRUE		*FALSE*				
2	Digital identity is only relevant in government programmes (like national IDs)	1 4%		25 96%				26
		0	*0–25%*	*25–50%*	*50–75%*	*75–100%*	*Other*	
3	I am in control of my digital identity (0 – min; 100 – max)	0 0%	13 57%	7 30%	3 13%	0 0%	0 0%	23
		Yes	*Maybe*	*No*	*No idea*			
4	Digital identity data should have economic value	13 46%	6 21%	6 21%	3 11%			28
		TRUE		*FALSE*				
5	There is equitable risk and reward sharing in digital identity systems	7 27%		20 77%				27
		The future of the internet	*An umbrella term for inter-related emerging digital technologies*	*Marketing jargon*	*Nothing*			
6	What does the metaverse mean to you? (multiple answers allowed)	7 22%	13 41%	12 38%	0 0%			32
		Gaming	*Concerts and exclusive screenings/ unveiling of products*	*Work environment*	*Other*			
7	Where have you experienced metaverses? (multiple answers allowed)	16 43%	10 27%	3 8%	8 22%			37

Table 2 Workshop scenarios summary

Scenario	*Summary*	*Questions for the group*
Scenario 1: Influencers in the metaverse	• Selena, 21 y.o. fashion icon with 10M+ followers across social media platforms • Promotes local Mexican textiles. • Meta rolling out their metaverse that consolidates Facebook, Instagram, Threads. • Metaverse to have AI influencers. • Selena"s business model in jeopardy and must consider how to react to these changes.	• What impact does the metaverse have on Selena's professional and personal digital persona? • What initiatives could Meta introduce to ensure influencers like Selena can continue to utilise its platform, while also expanding its own influencing capabilities with NPCs? • What strategies can Selena employ in the new metaverse in order to realise its benefits?
Scenario 2: working in a corporate metaverse	• Ramesh, design engineer in a construction company. • Company rolling out Google metaverse to aid design (digital twins, analytics, AI driven backlog analysis). • XR technologies and data driven logs may affect Ramesh at work and invade personal spaces.	• What unique opportunities exist for Ramesh from the deployment of the metaverse? • What risks exist for Ramesh? How can they be mitigated? • What considerations should the organisation have while implementing metaverse technologies in employee homes? • What considerations should the organisation have while deploying their metaverse solutions?
Scenario 3: Seeking healthcare in a public-private metaverse	• Sameera navigating a disjointed healthcare ecosystem while dealing with endometriosis and chronic pain. • NHS rollout of health metaverse in partnership with Palantir and DeepMind. • Metaverse could improve overall patient experience but also introduce risks of privacy infringement, data loss, and loss of ability for patient to discuss lived experiences.	• What opportunities does the new healthcare metaverse provide for Sameera? • What considerations should Sameera have regarding her health eID? • What considerations should the NHS have while deploying the metaverse? • What initiatives should Palantir consider while building and maintaining the technological infrastructure? • What responsibilities should DeepMind consider in their role within the ecosystem? What interventions, if any, should they deploy to meet these responsibilities? • What considerations should health services participants (doctors, healthcare professionals) have while accessing the health metaverse?

Table 3 Finding within the case study

ID	*Scenario*	*Finding within the case study*	*Why it matters*	*Links to Table 3*	*Links to Table 4*
S1-F1	Scenario 1	New commercial opportunities arise through transnational reach, digital fashion markets, and monetisation of a professional NPC identity.	Adoption is not only pressure from the platform; it also opens new market formats and business models.	C3	T2; T4
S1-F2	Scenario 1	Human authenticity is both a competitive advantage and a vulnerability: Selena's human presence differentiates her from AI, but expansion may also be read as 'selling out'.	Identity becomes an economic asset while authenticity becomes fragile and reputationally risky.	C5	T1; T2
S1-F3	Scenario 1	Personal/professional and public/private boundaries are difficult to maintain in immersive environments.	The notes suggest that identity separation in the metaverse is optimistic, raising privacy and reputational risks.	C1; C2	T1; T3
S1-F4	Scenario 1	Ownership of digital identity and AI-generated content is unclear.	The case raises unresolved questions about who owns data, persona-derived content, and labour captured by AI systems.	C4	T2; T3
S1-F5	Scenario 1	Platform incentives are structurally commercial, especially advertising-driven, producing distrust and cynicism about the metaverse as a social space.	User and influencer interests may be misaligned with the platform's commercial model.	C3; C4	T2; T3
S2-F1	Scenario 2	Immersive work tools offer genuine task-level benefits: 3D modelling, digital twins, better collaboration, and potentially better design decisions.	The value of XR is strongest where it directly improves technical work.	C3	T2; T4
S2-F2	Scenario 2	Tacit, human, and contextual labour is converted into hard metrics, performance scores, and AI-readable process data.	Quantification may increase efficiency, but it can also distort evaluation and remove nuance, creativity, and slack from work.	C5	T2; T4
S2-F3	Scenario 2	The employer's monitoring infrastructure extends into the worker's home, potentially capturing family members, room data, movement, and voice.	The work/home boundary collapses; surveillance no longer stops at the workplace.	C1; C6	T1; T3

Table 3 Finding within the case study (continued)

ID	*Scenario*	*Finding within the case study*	*Why it matters*	*Links to Table 3*	*Links to Table 4*
S2-F4	Scenario 2	Ownership and scope of capture expand from work product to telemetry and behavioural traces.	The notes question whether firms own not only output, but also surrounding data generated in the course of work.	C4	T2; T3
S2-F5	Scenario 2	Mitigation requires governance rather than trust alone: data minimisation, time limits, worker visibility into monitoring, and collective advocacy.	The notes frame regulation and worker voice as necessary counterweights to employer power.	C2; C4	T3; T4
S3-F1	Scenario 3	Immersive health systems could integrate fragmented records and generate research benefits, especially for understudied conditions such as endometriosis.	The case contains a real public-interest upside, not just risk.	C3	T2; T4
S3-F2	Scenario 3	Health-metaverse data intensifies vulnerability: bias, insurance discrimination, cascading harms, and intimate exposure become more likely.	Harms are amplified because the data is sensitive and the subject is already in a position of need.	C1; C6	T1; T4
S3-F3	Scenario 3	Consent is weak in practice because the ecosystem is complex, opaque, and difficult to challenge once harm has occurred.	Withdrawal of consent appears too late to be an effective safeguard.	C2; C4	T3
S3-F4	Scenario 3	Cross-border data flows, vendor partnerships, and unclear ownership create accountability gaps for NHS, Palantir, and DeepMind.	Governance complexity makes responsibility difficult to assign when something goes wrong.	C4	T2; T3
S3-F5	Scenario 3	Immersive healthcare risks privileging data over the patient, and avatars may blur who is qualified, real, or accountable.	The system may weaken professional judgment and patient trust if design centres data capture rather than care.	C5; C6	T1; T4

Table 4 Common finding across case studies

Common ID	*Common finding across case studies*	*How it appears across the three cases*	*Built from Table 4*	*Links to Table 4*
C1	Immersive systems expand data capture beyond ordinary boundaries.	In scenario 1, identity and content become continuously mineable; in scenario 2, homes and families become legible to employers; in scenario 3, intimate health and behavioural data are exposed in greater depth.	S1-F3; S2-F3; S3-F2	T1; T3
C2	Consent and transparency are inadequate safeguards.	All three cases question whether people really understand what is collected, how it is used, and whether consent can be meaningfully withdrawn after the fact.	S1-F3; S2-F5; S3-F3	T1; T3
C3	The technology offers genuine utility, but benefits are unevenly distributed.	Influencers gain market access, engineers gain better collaboration tools, and patients/research systems may gain better insight; yet platforms, employers, and vendors often capture the larger strategic value.	S1-F1; S1-F5; S2-F1; S3-F1	T2; T4
C4	Ownership, responsibility, and accountability are unresolved in multi-actor ecosystems.	Each case asks who owns the data or outputs, who is liable for misuse, and how responsibility is allocated across platforms, employers, vendors, and public institutions.	S1-F4; S1-F5; S2-F4; S2-F5; S3-F3; S3-F4	T2; T3
C5	AI, metrics, and avatars can displace or distort human judgment and identity.	Scenario 1 questions whether AI/NPC influencers will outperform humans; scenario 2 shows quantification reducing nuanced labour to metrics; scenario 3 warns that clinicians may default to data and that avatars can blur authenticity and trust.	S1-F2; S2-F2; S3-F5	T1; T2; T4
C6	Risks fall hardest on those with less power or higher vulnerability.	In scenario 1, marginalised groups may face exclusion and weak protection; in scenario 2, workers and their families have limited control; in scenario 3, patients face intimate, cascading harms and access barriers.	S2-F3; S3-F2; S3-F5	T1; T3; T4

Following the workshops the note takers and facilitator met up for a briefing and evaluation of notes taken. This allowed for clarification of understanding on any notes and a standardisation of note capture as well. The note taker's role is not to be the spokesman for the groups, but rather an analyst of the situation, considering the implications, actions and reactions of the actors and their effects on that given context (Thiollent, 2011). Notes were then sent to the facilitator. The facilitator (primary author

of this paper) then carried out a thematic analysis of the notes. First an in-scenario analysis was done, which identified and converted importing findings within each case study scenario into themes. Following that a cross-case study analysis was done. This practice highlighted the commonality across scenarios. This allowed for generation of common themes that aided in generalisation and connection back to academic literature (Costa et al., 2016). Abductive logics of inquiry have been applied to data collection and interpretation as it helps explain concepts in multiple layers: through an interrogation of knowledge that is shared, and through the reflexive practice that unearths further motivations that lie behind initial data collection.

Table 5 Emergent themes

Theme ID	*Emergent theme*	*What the theme means*	*Built from Table 3*	*Trace back to Table 2 examples*
T1	Boundary collapse	The metaverse erodes boundaries between public/private, work/home, body/avatar, and person/platform. Identity is no longer neatly separable from environment or system.	C1; C2; C5; C6	S1-F3; S2-F3; S3-F2; S3-F5
T2	Datafication redistributes power and value upward	The strongest pattern is not just innovation, but the conversion of identity, labour, and health into data assets that platforms, employers, and vendors can monetise or operationalise.	C3; C4; C5	S1-F1; S1-F4; S1-F5; S2-F2; S2-F4; S3-F1; S3-F4
T3	Governance lags behind immersion	Legal and organisational tools such as consent, ownership rules, liability, jurisdiction, and transparency are not keeping pace with immersive, networked systems.	C1; C2; C4; C6	S1-F4; S2-F5; S3-F3; S3-F4
T4	Human-centred design is the missing condition for legitimacy	Across all three cases, the technology is most defensible when it augments human judgment, dignity, inclusion, and advocacy rather than replacing them with optimisation alone.	C3; C5; C6	S1-F1; S2-F1; S2-F5; S3-F1; S3-F5

Table 2 provides a summary of each scenario. Detailed descriptions of each scenario can be found in the Appendix. All scenarios were fictitious for discussion purposes. Tables 3–5 provide a detailed description of how coding was done post workshop. Table 3 summarises case specific findings (F-codes), Table 4 then highlights common findings (C-codes) and finally Table 5 provides the higher order themes (T-codes) that were developed across case study findings.

4 Findings

4.1 Scenario 1: Influencers in the metaverse

Scenario 1 covered the dilemmas of Selena, a Mexican fashion icon who has amassed a considerable fan following on social media platforms by promoting local and national textiles. Selena, however, is faced with an emerging challenge: Meta launching its own metaverse that will consolidate all its platforms under one experience. Along with this shift, Meta plans to roll out new AI-generated influencers in the metaverse. Participants were asked to consider how these changes affect Selena, her personal and professional identity as well as how digital identity risks in this environment can be mitigated.

The scenario uncovered the limited avenues of control Selena was offered. Her digital identity and success as an influencer, carefully curated by her, are now at risk due to system changes. While she may try to keep control over her persona through what she posts on social media, the spaces for identity realisation and growth are limited to what the metaverse allows. Her livelihood is now in direct competition with AI. Participants recognised this issue and felt an underlying discomfort regarding the situation. Points were raised on how Meta, as the system administrator, was incentivised to drive scale and efficiency, whilst not having to prioritise the rights realisation of its participants. As all digital data is recorded, Selena's own data could be used to train AI into becoming automated influencers, without compensating Selena in any way. Participants recognised Selena's limited choice in whether to accept or resist a transition to the metaverse. She will have to compete in this newer, more complex marketplace. She may even find it harder to separate her personal and professional identity in the metaverse, as identity credentials may be consolidated.

Participants identified an opportunity for mutual benefit. AI-generated influencers could be used as a product offering, an extension of human influencers (like Selena), allowing humans to scale their reach, earning potential and be available 24/7. This could also provide an opportunity for better separation of professional and personal life. While this is a novel idea, it does raise considerable challenges. First, the outsourcing of identity and personal ethical values to AI. The AI bot can be co-opted for the spread of misinformation and possibly implicate Selena in transactions that her values do not align with. In fact, recent instances of identity fraud using deepfake technologies have indicated that this is already a considerable risk and can lead to financial losses as well as the spread of misinformation (Elliards, 2024; Leng and Ho-him, 2024; Thomas, 2024). Secondly, it may create distrust in the overall ecosystem if users are unsure whether they are interacting with human influencers or AI extensions of their human influencers. Participants recognised that deep-seated commercial interests of the scenario created a possible limitation in adoption or a cynicism in its usage beyond entertainment.

In seeking to address the risks and loss of agency for Selena, participants suggested the development of transnational frameworks to help develop normative principles of engagement in the metaverse, and balancing Meta's commercial interests with the expected civic requirements of human rights realisation. Participants suggested that Meta needed to provide clear guidance on the impact the metaverse would have on digital identities, in particular, how data was processed, and how participants could clearly define private spaces. Clear guidance on data ownership was required: who owns the personal data, who monetises it, clarity on what data was used to train AI bots and how those benefits are shared.

4.2 Scenario 2: Working in a corporate metaverse

Scenario 2 focuses on the professional identity mediation of Ramesh, a design engineer participating in a corporate metaverse rollout. The metaverse rollout is aimed at providing remote design teams the opportunity for collaboration while also collecting data to improve business decision making, measure staff efficiency, and assess team effectiveness. To engage with the metaverse, staff have been provided with XR and IoT devices that are now in Ramesh's home environment, thereby making the home environment part of the work environment.

Participants recognised the potential benefits of the metaverse rollout. It provided an opportunity for the organisation to gain deeper insights into the design process, provide collaborative technologies, and bring real-time data closer to designers to help in their design choices. Ramesh could benefit from engaging with prototypes in three dimensions, which would make him and his team more effective in their roles. However, this program created a vehicle to quantify and measure every activity of a professional. Embedding XR and IoT devices in a home setting may blur the lines between personal and professional interactions and spaces. It creates an environment of constant surveillance while viewing worker output and activity in terms of cost efficiency. It may also lead to a measurement bias, where quantified metrics such as turnaround times are given priority over creativity and architectural novelty, the latter of which may be more important for the design process.

Ramesh may have a limited locus of control in terms of privacy and identity management. Family members may show up in his XR device backgrounds, and even when he is not logged in, the activity (and inactivity) log can be used as a measure of his productivity. Coupled with this is an unclear understanding of data ownership. Not only can work content be captured, but content on daily logins, as well as spatial data of a home environment, is also captured. Context-devoid data analysis may create misguided expectations of the 'average employee' or the 'average productivity output' against which employees are measured.

Participants discussed a variety of solutions to address the above risks. Regulatory interventions may help reduce some risks of privacy infringement and allow employees avenues for personal data ownership. Although it was not clear how said rights could be exercised or how they interacted with future employment contracts that may have clauses for data collection. Employee unions were suggested as a means to collectively manage employee welfare in the face of exploitation and datafication risks. Overall, the discussion on avenues for governance focused on balancing power and control. Through collective action, participants envisaged the possibility of creating spaces for employees to better understand what data was being collected on them and how it was being used. It could also provide avenues to contest and contextualise data collection.

Work products are typically owned by organisations; however, in the context of metaverse technologies, this definition requires further investigation. If XR technologies, via telemetry, capture more than the work process or product, would that also be the company's to own? Participants considered this issue as something collective action could address through the development of policies and procedures of fair data use.

4.3 Scenario 3: Seeking healthcare in a public-private metaverse

Sameera suffers from endometriosis, a condition that has caused her debilitating pain for many years. She has seen many medical professionals (GPs, specialists, dieticians, and mental health professionals) as the condition has affected her physical and psycho-social wellbeing. The siloed NHS environment has meant that she has not been able to receive holistic support for her condition. The NHS now plans to roll out a health services metaverse in collaboration with Google DeepMind and Palantir. The system will provide a single database for patient data as well as link all medical service providers and insurers under one system. DeepMind will use the patient database to identify population trends and subsequently data-driven solutions to the NHS, service providers, pharma companies and insurers.

Participants analysed this scenario from the perspective of its different stakeholders: Sameera, NHS, Palantir and DeepMind, and healthcare professionals. Participants recognised the complexity of the ecosystem and the divergent stakeholder interests at play, at the centre of which lay an understanding of a patient's digital identity, specifically associated with their physical and mental well-being. The healthcare metaverse promised to consolidate disparate data sources, thereby making the patient's condition transparent, but did so in a way that made the process of data collection, usage, and sale opaque.

The scenario provided an opportunity for Sameera to gain holistic care for her condition and no longer must deal with fragmented health records and divergent healthcare professional recommendations. It could improve her overall patient experience and possibly lead to greater research into an understudied and underfunded health condition. However, concerns were raised on which entities had data access to personal health records. Private entities, like Palantir, could analyse and trade this data for financial benefit. Additionally, anonymisation techniques are often imperfect, making it a risky proposition for an individual like Sameera who would bear the risks of data theft. Participants suggested that Sameera's locus of control was limited to withdrawing consent in the case of data breaches, even though this would not compensate for any personal losses. Data loss across the health system could create significant risks for vulnerable populations.

Participants raised the need for clearer guidelines on data processing practices, including who had access to the data and how it would be used. As private enterprises like DeepMind and Palantir are transnational organisations, this raised concerns over the ability to implement effective regulatory jurisdiction over their entire business practices. Even with regulation in place, like the GDPR, companies may use the research in public interest clause as a legal basis for data processing. Regulatory sandboxes were proposed as a staged mechanism to understand the regulatory environment and build capacity within the government as well as the ecosystem partners. Additionally, a fiduciary responsibility model was proposed to commit ecosystem to partners to support the overall ambitions of better patient outcomes and personal data privacy, not just a profit maximisation status.

The NHS, as the system administrator, was considered to have significant responsibility for maintaining trust across the system. The NHS must provide transparency on data management practices and ensure consent was informed and understood. Additionally, it was required to find effective methods to govern the practices of its transnational partners that ensured a reduction in harm and limitation of

data transfer. The NHS would be required to enforce rules and monitor misuse. It would also require assistance in educating the public on how to interact in this space.

This scenario highlighted a unique opportunity for patients to gain easier access to health professionals, while also highlighting risks such as being diagnosed by digital data points, while ignoring the patients lived experiences. The healthcare specialist's role must expand to consider the role of documented data as well as incorporate patient feedback. Connected devices (like heart-rate monitors) may provide spurious insights that can lead to misdiagnosis. This requires a significant change in healthcare specialists' knowledge development, to not just be medical professionals but also to be adept in data management and data science.

In evaluating the scenario, participants became aware of the deeply complex environment, divergent stakeholder interests and the opacity of the overall system. While the system provided considerable benefits to patients, it highlighted a need for multi-stakeholder engagement to address its risks.

4.4 Thematic inferences

In-depth analysis of each case study brought about thematic findings, which are discussed in this section. Participants recognised the networked nature of the metaverse and how technologies owned by different partners with differing incentives needed to come together to provide an immersive experience. Through this analysis, participants raised concerns about the participation of for-profit companies in the datafication of personal life. In scenario 2, the corporation's incentive to drive efficiency gains meant Ramesh's home environment became part of the dataset used to analyse for efficiency. In scenario 3, the involvement of DeepMind and Palantir in personal health data collection and analysis meant that this data could be sold in markets to maximise company profits. Through this layered analysis of metaverse stakeholder groups, participants recognised that, through the datafication of their personal and professional lives, individuals (as users, employees, patients) were made transparent, while the system administrators and contracting service providers were made opaque. It became unclear who was responsible for data management, who benefited from its processing, and how an individual could understand and mitigate the risks they were exposed to in the metaverse. This created an overall sense of distrust in the system. Added to that was a concern about not knowing whether an individual was talking to a real person or an AI bot. Participants expressed concerns about the lack of affordances for managing their digital identity in each use case and the limited options for recourse and discussion presented in each case.

The metaverse drives a requirement for changing job descriptions and expectations of participating entities. Scenario 3 highlights this with the changing requirements of the NHS and doctors. The NHS, as the health system administrator, is required to create an environment that promotes trust and safety for its participants. Not only does the NHS need to consider health outcomes of its patients, but in the metaverse, it needs to consider how to promote a trustworthy environment for patient engagement, how to ensure transparency of data management practices, and how to hold its partners accountable to meet expected safety, security, and privacy expectations. Doctors are required to learn data science skills and balance insights generated from datafication with the lived experiences of individuals. Private sector participants, such a Palantir and DeepMind, may need to be held accountable for societal outcomes of health and patient

confidentiality and not just for shareholder return. Scenarios 1 and 2 highlighted the limited autonomy users (influencers, employees) have in the face of systemic changes. While data consent may provide some control over what data is shared in the metaverse, it cannot challenge the structural changes being imposed. Trust in the metaverse is thus crucial to drive adoption and continued growth. This requires system administrators and service providers to build an environment for trusted transactions and interactions that allow participants to engage and push for equitable risk-reward sharing. This could be through the development of transnational agreements, effective terms of service policies and practices, and user engagement forums as avenues for ongoing review of participant welfare.

Participants highlighted the lack of control and data ownership in the metaverse. Consent, while a possible avenue for data control, may be limited in use cases like a healthcare metaverse, where data processing in the name of public services may continue to happen. In a corporate metaverse, consent may play a limited role as the work product and process for making that product could be entitled as the corporation's ownership. If consent is revoked, after data collection, it was unclear on whether past data could be removed and if so, were there abilities to remove it from all partnering entities. On the other hand, any personal data loss would put individuals at risk. Even in scenario 1, participants became aware that data generated on the platform may be used as AI-training data, without clear guidance on what data was or was not used. The lack of transparency on data processing practices was coupled with a consideration on lack of accountability risk within the metaverse. While regulation was considered important to define the expectations of partners, the effectiveness of regulation may not extend to transnational partners. Thus, the need for transnational regulatory frameworks to hold large transnational companies to account on expectations around privacy and data security.

In scenario 2, a useful prompt that helped focus the group was that, through the metaverse, employees were no longer going to work, but that work was entering the employees' homes. This thought helped anchor the group's discussion around how the metaverse poses risks to different aspects of private life. It is not just about device logins but the individual in the metaverse is constantly creating identity data by interacting with their environments and accessing metaverse services. Governing eID thus becomes a dynamic problem to solve in each use case, where we can no longer demarcate the lines between personal data and the environment or service provided and how these interactions change over time. Consent, already disputed in its efficacy, becomes an even weaker control as users are consenting to constant data capture. This issue extends beyond the need for transnational regulatory frameworks to the issue of personal autonomy in emerging digital spaces. It points to the requirement to move away from regulation anchored on data classification which may prove ineffective in such environments and refocus regulation towards end-user safety from harms.

5 Recommendations

This study highlights the complex environments that metaverses encompass. To make the experience immersive, metaverses integrate multiple technologies into a single experience through a vast network of technological and commercial arrangements. An individual's identity extends beyond their identifying characteristics (usernames, passwords, logins) to encompass the relationships (interactions with services) and the

affordances in the environment (the metaverse as a whole). In a dynamically rendered environment, digital identity trails are constantly created, and the ownership and control of this data is contested. The challenge of eID governance in the metaverse is in ensuring that, through this exercise, the individual has the opportunities required to realise their rights and identity aspirations. This section lays out a set of recommendations that can be incorporated into metaverse to improve transparency, increase end-user participation and thereby reduce risks and harms from their usage.

5.1 Value-sensitive design to support system development

This study highlights the importance of considered system design, as it creates the affordances for participants. Not bringing participants into the design process creates system distrust and may lead to a lack of adoption. Consultation on system design can surface opportunities for identity management early and be captured in the design process. Anand and Brass (2021) highlight three key interventions in the design process: identification and engagement with direct and indirect stakeholder groups, articulation of values for each stakeholder group, and the incorporation of value-sensitive design principles in the system development process. As found in this study, participants may struggle to understand the environment the metaverse creates, so consultation sessions can be used as a means of educating on the technologies being designed in a controlled environment. This allows users to appreciate the transformative nature of the technologies and meditate on the risks, controls, and questions they may have about the environment. Value-sensitive design adopts a tripartite methodology: conceptual, empirical, and technological investigations (Friedman et al., 2013). The conceptual framework provides a philosophical foundation for identifying the 'right' segments of stakeholders (direct and indirect) and the values that are important to each. The empirical assessment evaluates the validity of conceptual frameworks and examines stakeholder priorities and trade-offs through in-depth interviews and focus groups. The technical assessment evaluates the technology itself and the choices that enable the implementation of a value hierarchy identified through conceptual and empirical studies. When applied to the different scenarios and stakeholder segments in this study, value-sensitive design provides a robust foundation for building a socio-technical infrastructure that supports multistakeholder needs. When considered within the context of the scenarios, it offers Sameera, Ramesh and Selena options to engage with the transformative technological changes being imposed on them and the ability to voice their concerns and highlight the values that are important to them. It allows for the development of design choices that support identity ownership (opt out from AI training), professional-personal life datafication, and the ability to better understand the potential benefits of digitalised identity health records for an individual beyond the abstractions of population-based benefits.

5.2 Regulation anchored on human rights realisation

Current regulation – data protection and data privacy – are anchored on two important tenets. The first is an ability to separate data into categories of personal versus non-personal, sensitive versus non-sensitive, identifiable versus anonymous. The second is the assignment of data controller responsibility to a clear entity. In the metaverse both

paradigms are challenged. Metaverses may capture a continuous stream of hyper-personal data; be that biometric information (eye tracking, heart rate), interactions (textual, verbal, emotional, voice inflections), and data that provides insights into a personal environment or violates the privacy of those around (such as Ramesh's family). As highlighted in Sameera's scenario the assignment of responsibility too becomes unclear. The networked environment creates a 'many hands' problem where it becomes hard to assign responsibility for responsible data processing activities.

New approaches in digital regulation are required that centred on the safety of the individual and anchored on human rights realisation. These approaches need to consider the risks and harms that digital environments may present to the individual and provide clear regulatory safeguards that protect the individual. A rights-based approach would then filter through the lifecycle of the digital environment – mandating interventions such as privacy-by-design through system lifecycle, make complex digital environments easily explainable and auditable, prioritise civil society participation in system governance, place moratoriums on contested technologies (live biometrics, emotional recognition technologies) and conduct ongoing human rights impact assessments (HRIAs) to assess system compliance to regulatory intent. It would also provide clarity on the expectations and accountabilities of system administrators and service providers in ensuring environments are kept safe for individuals.

Additionally, just as GDPR has found momentum as the blueprint for data protection regulation, a similar commitment is required from governments to manoeuvre towards enforceable transnational rights-based regulation to ensure transnational platforms can be held accountable to human rights objectives.

5.3 Building multi-layered governance strategies

In addition to regulatory interventions, multi-layered governance strategies are required to build trust and transparency in the metaverse environment. The aim of such interventions would be to set a clear set of practices and norms for metaverse use cases. These guidelines set the guardrails for acceptable practices for all system participants. A tiered model for hard and soft governance interventions is required: that covers macro level national and transnational regulatory frameworks, standards and certification boards, as well as values-based funding bodies to micro level interventions such as embedding social science researchers in design teams and continuous education of developers to challenge techno-deterministic epistemologies. Regulatory sandboxes provide controlled environments for capacity building in the operations and enforcement parties, and opportunities to identify evolving risks from emerging technologies (Attrey et al., 2020). It also allows companies to market test innovations, reduce regulatory uncertainty and possibly improve financing for start-ups by showcasing market test results.

This study also highlights the increased expectation from eID system administrators and service providers to build transparent and responsible procedural governance practices. The expectations from service providers, such as DeepMind and Meta, are not just of profit maximisation but also of creating safe environments for their end-users. This can be achieved through formalised processes, such as sector specific regulations or the invocation of fiduciary responsibilities on such entities, and through informal processes, such as transparency statements and HRIAs. Additionally, there are expectations from system administrators and specialist service providers, such as the

NHS and its medical professionals, to develop new skills. While findings from large language models and data science are extremely relevant, they require specialists to be able to balance these findings in light of a person's lived experiences that can be unique.

New models for data ownership – such as data cooperatives – provide a means for collective bargaining as well as new business models for data monetisation. Collective action, through user group alliances or unions, may assist in balancing power amongst stakeholders in the system and negotiating for greater pathways for rights realisation of users.

5.3 Moving beyond volumetric measures of success

In considering the realisation of human rights in metaverse systems, it is essential to consider normative rights of identity and privacy realisation while also making design considerations that are culturally and contextually relevant. If immersive and dynamic digital environments, like metaverses, become dominant technologies for accessing essential services like healthcare, it becomes necessary to consider who can access these services and who gets excluded. Anand and Brass (2021) explain three dimensions to consider: ethical, experiential, and exclusionary. Ethical assessments help investigate how fundamental human rights are realised through eID systems. Experiential assessments may investigate the lived experiences of people when faced with eID systems, critiquing the impact said systems have on human agency. Exclusionary assessments examine participation rates across demographics and the underlying causes of lags in specific segments. These assessments provide a way to look beyond basic volumetric reports of system adoption and understand the underlying impact the metaverse may be having on different user segments. It helps showcase who benefits, and who is being left behind. Additionally, it may provide findings that impact system design and governance strategies, such as how a healthcare metaverse can realise the right to identity and access to health services while maintaining the user's right to privacy. In designing fairer systems, it is thus important for individuals to be able to review and contest large language model-based outcomes as well as provide first-person feedback.

6 Conclusions

The metaverse is the new imaginary of an immersive digital environment, where individuals do not just participate through two-dimensional screens but are part of a dynamically rendered environment that they can interact with. In metaverses, digital identity is constantly created. Individuals are constantly tracked through their active and passive interactions within the metaverse, whether that is through their own actions or through the sensors embedded in their lived environment. In this sense, governing digital identity needs to move beyond strategies anchored in categorisations of personal and sensitive data, to more dynamic strategies that improve user understanding of the metaverse, support user participation and build trust in the system.

By delving deeper into use cases of the metaverse, this research unearths the need for a broader conceptualisation of digital identity. Digital identity in the metaverse has distinct spatial, temporal and relational aspects to it. eID data can be created through identity credentials (and credentialing systems), avatars in the system, IoT and spatial

data, as well as data generated by constant interactions between the user and the dynamic metaverse environment. This novel framework considerably expands the academic and practitioner understanding of digital identity. It also expands the avenues for governance of eID systems that need to move beyond technical fixes and consider the expanded socio-technical experience of the metaverse.

This study highlights that the path to digitisation of the human experience is not a static one. It will continue to grow and expand with ever increasing and invasive technologies. Digital identity is not just about the login credentials but the continuous extraction of identity traits in digitised worlds. In the process of datafication, human rights become a casualty, and human subjectivity is supplanted by supposed 'objective' data attributes which can be used for analysis, optimisation and economic value creation. The current paradigms of eID governance (regulation, consent, fair use) are ineffective in such environments. This research underlines the need for a fundamental rethink in how eID systems should be conceptualised and subsequently governed by keeping the realisation of human rights as the central objective. This research has discussed a variety of such instruments, such as rights-based regulation, HRIAs, participatory design practices and the use of collective action forums achieve this goal. It has highlighted a need for greater partnership to also ensure that interventions can be enforceable across national boundaries. Overall, in the face of more complex digital environments this study pushes for greater end-user participation and organisational accountability as key tenets in achieving the value from frontier digital environments, while also addressing their inherent risks.

7 Limitations

The use of three hypothetical scenarios may not fully capture the diverse real-world situations of digital identity deployment. The participant group, consisting mainly of young adults from a public administration program, limits the perspectives represented, excluding older users and marginalised communities. Additionally, rapid technological advancements in the metaverse may make some findings outdated. Lastly, the study focuses on broad governance principles without delving into the specifics of regulatory frameworks or regional cultural differences.

8 Future research directions

Future research on digital identity governance in the metaverse should focus on several areas. Expanding studies to include diverse participant groups across different ages, industries, and cultures will offer a more comprehensive understanding. Ethical concerns like identity commodification, data privacy, and algorithmic bias need exploration, alongside the creation of tailored ethical frameworks.

Comparative studies on governance approaches across jurisdictions could inform global best practices, while interdisciplinary research from law, sociology, engineering, and economics can provide holistic solutions. Longitudinal studies tracking digital identity evolution over time would offer deeper insights.

Declarations

All authors declare that they have no conflicts of interest.

References

Anand, N. and Brass, I. (2021) 'Responsible innovation for digital identity systems', *Data & Policy*, Vol. 3, p.e35, DOI: 10.1017/dap.2021.35.

Attrey, A., Lesher, M. and Lomax, C. (2020) 'The role of sandboxes in promoting flexibility and innovation in the digital age', *Going Digital Toolkit Notes*, Vol. 2), https://doi.org/10.1787/cdf5ed45-en.

Bloomberg (2021) 'Metaverse may be $800 billion market, next tech platform', *Insights*, Bloomberg Professional Services [online] https://www.bloomberg.com/professional/blog/metaverse-may-be-800-billion-market-next-tech-platform/ (accessed 29 July 2023, 16:08:23).

Bradbury, D. (2021) *De-Identify, Re-Identify: Anonymised Data's Dirty Little Secret*, September [online] https://www.theregister.com/2021/09/16/anonymising_data_feature/ (accessed 11 May 2024, 12:21:45).

Brass, I. and Sowell, J.H. (2021) 'Adaptive governance for the internet of things: coping with emerging security risks', *Regulation & Governance*, Vol. 15, No. 4, pp.1092–1110, https://doi.org/10.1111/rego.12343.

Cerasa, A., Gaggioli, A., Marino, F., Riva, G. and Pioggia, G. (2022) 'The promise of the metaverse in mental health: the new era of MEDverse', *Heliyon*, Vol. 8, No. 11, p.e11762, https://doi.org/10.1016/j.heliyon.2022.e11762.

Clarke, R. (2019) 'Risks inherent in the digital surveillance economy: A research agenda', *Journal of Information Technology*, Vol. 34, No. 1, pp.59–80, https://doi.org/10.1177/0268396218815559.

Costa, C., Breda, Z., Pinho, I., Bakas, F. and Durão, M. (2016) 'Performing a thematic analysis: an exploratory study about managers' perceptions on gender equality', *The Qualitative Report*, https://doi.org/10.46743/2160-3715/2016.2609.

Davis, D.Z. and Chansiri, K. (2019) 'Digital identities – overcoming visual bias through virtual embodiment', *Information Communication and Society*, Vol. 22, No. 4, pp.491–505, Scopus, https://doi.org/10.1080/1369118X.2018.1548631.

Deloitte (2022) *What's all the Buzz about the Metaverse?* [online] https://www2.deloitte.com/us/en/pages/center-for-board-effectiveness/articles/whats-all-the-buzz-about-the-metaverse.html (accessed 27 August 2023, 11:32:22).

Dionisio, J.D.N., Iii, W.G.B. and Gilbert, R. (2013) '3D virtual worlds and the metaverse: current status and future possibilities', *ACM Computing Surveys*, Vol. 45, No. 3, pp.1–38, https://doi.org/10.1145/2480741.2480751.

Elliards, X. (2024) *AI Deepfake Video of John Swinney on Sky News Goes Viral on Twitter* [online] https://www.thenational.scot/news/24305685.ai-deepfake-video-john-swinney-sky-news-goes-viral-twitter/ (accessed 18 May 2024, 14:34:00).

Freeman, G., Zamanifard, S., Maloney, D. and Acena, D. (2022) 'Disturbing the peace: experiencing and mitigating emerging harassment in social virtual reality', *Proceedings of the ACM on Human-Computer Interaction*, Vol. 6, No. CSCW1, pp.1–30, https://doi.org/10.1145/3512932.

Friedman, B., Kahn, P.H., Borning, A. and Huldtgren, A. (2013) 'Value sensitive design and information systems', in Doorn, N., Schuurbiers, D., van de Poel, I. and Gorman, M.E. (Eds): *Early Engagement and New Technologies: Opening up the Laboratory*, Vol. 16, pp.55–95, Springer Netherlands, https://doi.org/10.1007/978-94-007-7844-3_4.

GDPR (2016) *Fundamental Texts on European Private Law*, Hart Publishing, https://doi.org/10.5040/9781782258674.

Goffman, E. (1959) *The Presentation of Self in Everyday Life (Repr)*, Penguin Books, London.

Greenleaf, G. (2019) *Global Data Privacy Laws 2019: 132 National Laws & Many Bills*, 8 February, 157 Privacy Laws & Business International Report, 14-18, Available at SSRN [online] https://ssrn.com/abstract=3381593.

Guo, E. (2022) 'A Roomba recorded a woman on the toilet. How did screenshots end up on Facebook?', *MIT Technology Review*, December [online] https://www.technologyreview.com/2022/12/19/1065306/roomba-irobot-robot-vacuums-artificial-intelligence-training-data-privacy/ (accessed 22 October 2023).

Hadi, R., Melumad, S. and Park, E.S. (2023) 'The metaverse: a new digital frontier for consumer behavior', *Journal of Consumer Psychology, JCPY*, Vol. 1356, https://doi.org/10.1002/jcpy.1356.

Hu, M. (2017) 'Biometric surveillance and big data governance', *The Camb. Handb. of Surveillance Law*, pp.121–149, Cambridge University Press, Scopus, https://doi.org/10.1017/9781316481127.006.

Jain, S. (2023) *PII Data Breach: Indian PII, Aadhaar IDs for Sale on Darkweb*, 25 October [online] https://thecyberexpress.com/pii-data-breach-sparks-concern/ (accessed 18 May 2024).

Leng, C. and Ho-him, C. (2024) *Arup lost $25mn in Hong Kong deepfake video conference scam*, 17 May [online] https://www.ft.com/content/b977e8d4-664c-4ae4-8a8e-eb93bdf785ea (accessed 11 May 2024).

Liu, H., Bowman, M., Adams, R., Hurliman, J. and Lake, D. (2010) 'Scaling virtual worlds: Simulation requirements and challenges', *Proceedings of the 2010 Winter Simulation Conference*, pp.778–790, https://doi.org/10.1109/WSC.2010.5679112.

Moncur, W., Orzech, K.M. and Neville, F.G. (2016) 'Fraping, social norms and online representations of self', *Computers in Human Behavior*, Vol. 63, pp.125–131, Scopus, https://doi.org/10.1016/j.chb.2016.05.042.

Paul, A. (2024) 'Watch a tech billionaire talk to his AI-generated clone', *Popular Science*, 1 May [online] https://www.popsci.com/technology/ai-clone-interview/ (accessed 18 May 2024).

Rao, U. (2018) 'Biometric bodies, or how to make electronic fingerprinting work in India', *Body and Society*, Vol. 24, No. 3, pp.68–94, Scopus, https://doi.org/10.1177/1357034X18780983.

RLTY (2022a) 'The top 5 biggest metaverse events trends so far in 2022', *Medium*, 10 August [online] https://rltylive.medium.com/the-top-5-biggest-metaverse-events-trends-so-far-in-2022-bafe00bab5c5 (accessed 18 May 2024).

RLTY (2022b) 'Why metaverse concerts are here to stay', *Medium*, 24 August [online] https://rltylive.medium.com/why-metaverse-concerts-are-here-to-stay-f9de1f4e3756 (accessed 18 May 2024).

Schoemaker, E., Baslan, D., Pon, B. and Dell, N. (2021) 'Identity at the margins: Data justice and refugee experiences with digital identity systems in Lebanon, Jordan, and Uganda', *Information Technology for Development*, Vol. 27, No. 1, pp.13–36, https://doi.org/10.1080/02681102.2020.1785826.

Schulenberg, K., Freeman, G., Li, L. and Barwulor, C. (2023) ''Creepy towards my avatar body, creepy towards my body': how women experience and manage harassment risks in social virtual reality', *Proceedings of the ACM on Human-Computer Interaction*, Vol. 7, No. CSCW2, pp.1–29, https://doi.org/10.1145/3610027.

Sobti, S., Sahni, B. and Bala, K. (2020) 'Surgical coverage of cataract in a rural area of north India: A cross-sectional study', *Journal of Family Medicine and Primary Care*, Vol. 9, No. 8, p.4112, https://doi.org/10.4103/jfmpc.jfmpc_520_20.

Solove, D.J. (2024) *Data Is What Data Does: Regulating Based on Harm and Risk Instead of Sensitive Data*, 21 January, 118 Northwestern University Law Review 1081 (2024), GWU Legal Studies Research Paper No. 2023-22, GWU Law School Public Law Research Paper No. 2023-22, SSRN [online] https://ssrn.com/abstract=4322198 or http://dx.doi.org/10.2139/ssrn.4322198.

Sullivan, C. (2016) 'Digital citizenship and the right to digital identity under international law', *Computer Law & Security Review*, Vol. 32, No. 3, pp.474–481, https://doi.org/10.1016/j.clsr.2016.02.001.

Sweeney, L. (2000) *Simple Demographics Often Identify People Uniquely*, Pittsburgh [online] https://dataprivacylab.org/projects/identifiability/paper1.pdf (accessed 18 May 2024).

Thiollent, M. (2011) 'Action research and participatory research: an overview', *International Journal of Action Research*, No. 2, pp.160–174, https://doi.org/10.1688/1861-9916_IJAR_2011_02_Thiollent.

Thomas, D. (2024) *WPP Boss Targeted by Deepfake Scammers Using Voice Clone*, 10 May [online] https://www.ft.com/content/308c42af-2bf8-47e4-a360-517d5391b0b0 (accessed 18 May 2024).

Tolentino, D. (2024) 'AI personas are the future of dating, Bumble founder says. Many aren't buying', *NBC News*, 10 May [online] https://www.nbcnews.com/tech/internet/ai-personas-are-future-dating-bumble-founder-says-many-arent-buying-rcna151738 (accessed 11 May 2024).

Williams, D.P. (2020) 'Fitting the description: historical and sociotechnical elements of facial recognition and anti-black surveillance', *Journal of Responsible Innovation*, Vol. 7, No. Sup 1, pp.74–83, https://doi.org/10.1080/23299460.2020.1831365.

Appendix

Workshop scenarios

Scenario 1: Influencers in the metaverse

Selena is a 21-year-old fashion icon that has built an influential presence in the digital space. Across the major social media applications – Facebook, Instagram, Snapchat, Twitch – her followership far exceeds 10 million people and her engagement scores (likes, clickthrough rates) continue to rise. Selena has worked very hard to create a social media presence that aligns with her style and values. She particularly has made a name in promoting Mexican clothing patterns to a global audience. Her fame has grown through promotion of Mexican textiles and championing fair pay to craftsmen, as well as the use of sustainable materials. As her fame has grown, global manufacturers have been interested in partnering with her. While this could be lucrative for her, it could also signal an abandonment of the principles she has cultivated online. Currently she continues to work with the national brands she has supported since the beginning of her career, although she is acutely aware of the potential loss in revenue and reach through this model.

Being digitally adept, Selena also manages to create a more private digital social space for herself where she can interact with close friends and family through private pages. Here she can be less guarded in her communication. Although this has not always been successful, as her fame rises tabloids increasingly try to invade her personal spaces both online and offline, thereby creating cracks in her well-maintained digital persona. In a recent scoop she was caught wearing a sweatshirt made by a large global clothing manufacturer that has sweatshops in Bangladesh.

Meta has just announced the formal rollout of their metaverse: a dynamic digital environment that is interactive and immersive. It brings together Meta's platforms (Facebook, Instagram, Threads) and XR technologies under one umbrella. This has meant that a single digital identity of a person can interact in the metaverse through different

mediums; be it using XR technologies, threads comments or Instagram pictures. Not only will the metaverse be a new experience for its users, but it will also be dynamically rendered and have many AI-generated capabilities, such as NPCs (non-player characters), that can be interacted with while navigating the digital space. Over time NPCs may also become brand ambassadors, doorkeepers, and AI-generated influencers for sponsored content. Meta also plans to connect its metaverse with other social media platforms and evolving metaverses. This would mean a single persona can travel from Meta's environment into platforms and metaverses like Twitch, Snapchat seamlessly.

Meta's announcement has significant impacts for Selena. The announcement brings significant opportunities for expanding her brand presence across the metaverse, but also creates concerns for her own privacy as well as increased competition.

Questions for the group

- What impact does the metaverse have on Selena's professional and personal digital persona?
  - a What opportunities and risks exist for Selena?
  - b What opportunities and risks exist for Meta with the new business model?
- What initiatives could Meta introduce to ensure influencers like Selena can continue to utilise its platform, while also expanding its own influencing capabilities with NPCs?
- What strategies can Selena employ in the new metaverse in order to realise its benefits?

Scenario 2: Remote working in a corporate metaverse

Ramesh works for a construction & engineering company, as a design engineer. Ramesh‟s job has, in the past, consisted of building and reviewing proposed constructions for the firm. This is an extremely technical job that brings together competing priorities of the business: safety and structural integratory of buildings, aesthetic appeal, construction expertise availability, and commercial considerations of cost and profitability. Ramesh enjoys the complexity associated with his role and the multi-dimensional demands he needs to deal with daily. His job is integral to a project's success but at times is a bottleneck when delivering against deadlines.

Since 2020 and in response to the COVID-19 pandemic, Ramesh has moved to a 100% virtual role. He communicates with his team via virtual meetings while also providing him the flexibility to spend time with his young family. It allows him the flexibility to pick up his kids from school in the middle of the day and spend time with them, before logging back in later in the day to finish his work.

Ramesh's company has partnered with Google to roll out a corporate metaverse and has been providing employees with XR devices. The first phase of the metaverse project has focussed on frontline workers and providing them with on-the-job training via augmented reality. This has really boosted worker productivity and reduced the costs of trainings in the company. Additionally, through the deployment of surveying drones and integrated site cameras overall safety on construction sites has improved as well.

The next phase of the company's metaverse project will focus on the design team. The project is expected to have four core priorities. First, the deployment of digital twin

capabilities. This will allow geographically dispersed design teams to engage on new project design using VR technologies; moving away from viewing designs in 2 dimensions, to being able to analyse 3D models remotely. Second, improving decision making through the deployment of analytical software. This will allow designers to see the real time impact of the design choices they propose on a project's expected ROI (return on investment). Third, time in stage analysis aimed at gaining greater transparency of the design process; identifying bottlenecks and escalating if time commitments aren't met. And finally, backlog analysis. As the entire process is now digitised, AI will be deployed on project design process data in order to improve efficiency in the future and judge employee performance. Design teams will be provided with VR devices, haptic feedback devices, as well as Google Nest for conferencing facilities as well as voice feedback commands in the metaverse.

While Ramesh recognises that this project has significant opportunities to improve his overall effectiveness of his job, he is also concerned with the surveillance risks.

Questions for the group

- What unique opportunities exist for Ramesh from the deployment of the metaverse?
- What risks exist for Ramesh? How can they be mitigated?
- What considerations should the organisation have while implementing metaverse technologies in employee homes?
- What considerations should the organisation have while deploying their metaverse solutions?
    a What risks exist? How can they be mitigated?

Scenario 3: Seeking healthcare in a public-private metaverse

Sameera suffers from endometriosis, a condition where tissue like the lining of the womb grows in other places of the body, such as the ovaries and fallopian tubes. This condition is frequently under-diagnosed in women and has significantly impacted Sameera's lived experience throughout her teenage years and adult life. It has caused her substantial physical pain during periods as well as daily discomfort while going to the toilet. Sameera has had to seek medical advice from many medical professionals: general practitioners (GPs) of the NHS, private care obstetricians & gynaecologists, and specialist surgeons. As the condition has developed over time, she has also had to see dieticians, dermatologists and mental health professionals as endometriosis also impacts psycho-social wellbeing.

As there is limited consensus on treatment, Sameera has had to provide her medical history to many professionals within the same field. Disjointed medical systems has also meant that medical histories are often not shared across providers, leaving Sameera to either fill in the gaps herself or get conflicting advice from professionals.

The NHS has planned to roll out a ground-breaking health systems metaverse in partnership with many private sector med-tech health providers including Google DeepMind and Palantir. A single patient database will be created and hosted by Palantir. All participating entities can access and update patient data once they have consent from the patient. Consent is provided through a key sharing system, as part of the NHS‟s new

digital health ID wallet. The new system also provides access to non-healthcare professionals such as dieticians, alternate medicine professionals as well as insurers. DeepMind provides an overlaying AI capability that will analyse millions of patient records to identify population trends, risks and subsequently solutions to the NHS, healthcare providers, pharma companies, insurers, and other participating entities.

The new model is expected to reduce the heavy patient burden currently on the NHS through a more streamlined process patient management. It will open the door to private sector engagement in healthcare management.

Sameera has been picked to participate in the phase 1 rollout of this service. She feels relieved that the new platform may make life simpler for her when engaging with the healthcare sector but also worried about the multi-stakeholder environment that she is now entering.

Questions for the group

- What opportunities does the new healthcare metaverse provide for Sameera?
- What considerations should Sameera have regarding her health eID?
- What considerations should the NHS have while deploying the new health metaverse?
- What initiatives should Palantir consider while building and maintaining the technological infrastructure?
- What responsibilities should DeepMind consider in their role within the ecosystem? What interventions, if any, should they deploy to meet these responsibilities?
- What considerations should health services participants (doctors, healthcare professionals) have while accessing the health metaverse?
- What responsibilities should insurers and pharma companies consider within the ecosystem?