frontiers | Frontiers in Virtual Reality

TYPE Hypothesis and Theory
PUBLISHED 05 February 2025
DOI 10.3389/frvir.2025.1401073

OPEN ACCESS

EDITED BY
James Harland,
RMIT University, Australia

REVIEWED BY
Hiroyuki Obari,
Aoyama Gakuin, Japan
Rahib Imamguluyev,
Baku Business University, Azerbaijan

*CORRESPONDENCE
Carl Hayden Smith,
csmith7@uel.ac.uk
Judith Molka-Danielsen,
j.molka-danielsen@himolde.no

†These authors have contributed equally to this work and share first authorship

RECEIVED 14 March 2024
ACCEPTED 15 January 2025
PUBLISHED 05 February 2025

CITATION
Smith CH, Molka-Danielsen J, Webb-Benjamin J-B and Rasool J (2025) The challenges of consent in a decentralised metaverse: exploring ethically informed protections and standards to safeguard humans.
Front. Virtual Real. 6:1401073.
doi: 10.3389/frvir.2025.1401073

The challenges of consent in a decentralised metaverse: exploring ethically informed protections and standards to safeguard humans

Carl Hayden Smith[1*†], Judith Molka-Danielsen[2*†], Jean-Brunel Webb-Benjamin[3] and Jazz Rasool[4]

[1]Department of Media in the School of Arts and Creative Industries, University of East London, London, United Kingdom, [2]Faculty of Logistics, Molde University College, Molde, Norway, [3]Djinn Technologies Ltd., London, United Kingdom, [4]Energy Diamond Consultancy Ltd., London, United Kingdom

Throughout the history of Web2.0 there is a large body of evidence of data being used for something other than what it was consented to be used for. What were 2D webpages are becoming 3D worlds, collectively forming a Metaverse of virtual and mixed reality domains which should help to create new interactive learning, social and economic opportunities. In this paper we reflect on how the physical world will itself become a networked interface, making reality even more machine-readable, click-able, and searchable. We begin with a review of the Metaverse and some of the consent challenges that arise and urgently need to be addressed whilst exploring its potential. There is a core need for creators of Metaverse environments to make them safe spaces for everyone to use. We explore and review the knowledge gap of consent needed to ensure a fair and just use of data within the Metaverse. We explore the challenges of consent including examples such as unauthorised surveillance and the need for ethical and moral standards in large platforms such as VRChat. This need is then further elaborated using experiences gathered during the XPRIZE Rapid Re-skilling Competition. The main contributions of this paper are the five stage Shared Consent Framework which was developed in response to understanding the limitations of existing consent frameworks and the extended definition of the Metaverse.

KEYWORDS

Metaverse, ethics, decentralised, consent, virtual reality, Artificial Intelligence

1 Introduction

A distinguishing component of the Metaverse is the merging of our representation and identity in the real world with a digital representation of ourselves in the digital world. Digital twins are formed as the virtual and the digital are connected through a network of sensors. The recent versions of the iPhone Max Pro with its inbuilt Lidar technology, as well as Apple's new mixed reality headset Vision Pro, can create a 3D point cloud of objects and the environment you are in. This large scale "scanning of the world" has direct impacts on our privacy. When Google Glass was released in 2013, it was banned in department stores as it was deemed an unacceptable invasion of privacy (Kozuch, 2022; Steele, 2019). Now however, depth sensors are being built into many types of devices, yet ethical mechanisms

for protecting our body-image and possessions have not been well established or kept up with the pace of emerging volumetric capture proliferation (Privacy and Human Rights Report, 2017). Welcome to the digital twinning of your personal context, a democratic way of utilising the senses or sensor extensions of them for future mixed reality experiences, something Alexander Bard has coined as "sensocracy" (Bard, 2020). By wearing a Mixed Reality headset such as the Microsoft HoloLens or Apple's Vision Pro you are by default generating 3D scans of everything you see, and that includes people. The issue is that once your body-image has been captured, it can be used against your knowledge, *ad infinitum* in deep-fake productions.

As a result of the pandemic, virtual production and volumetric capture studios are now in high demand, however, frameworks for how the products of these studios should be managed have yet to be formulated. The non-fungible token (NFT) or Smart Contract may play a role in the protection of body image, allowing ownership over our digital selves. The benefits of this include securing your fingerprint through smart contracting. This form of contracting can also be used to provide clear and valid ownership over personal skills and certificates that authorise them. Tokens related to personal purpose and identity have come to be known as "Soulbound" tokens (SBTs) (Exmundo, 2022; SSRN, 2022). SBTs are unique types of NFTs that cannot be moved, burned or sold from original crypto wallets. The SBT can be used to verify the identity of an individual. SBTs can be added to NFT metadata and as such can be used to validate a user's intellectual property (Ohlhaver et al., 2022). For example, with an embedded SBT, it would be possible to know when someone views a video of yourself. This hints at the need for a future where you own your own body scans before designers do, "design or be designed" a viewpoint covered by Daniel Fraga in his "Manifesto of Ontological Design" (Fraga, 2020).

However, issues of consent will expand exponentially once mixed reality headsets and contact lenses are more widely adopted. This is because, through the simple act of looking, we will be making "new realities with our eyes". Meta's Horizon, Unreal and Nvidia are some of the key players creating their own walled gardens of the Metaverse.

This paper will explore and review the knowledge gap that exists currently within consent frameworks to ensure a fair and just use of data within the Metaverse.

We will seek to answer the research questions:

1. What are the challenges of consent for a decentralised Metaverse?
2. What protections can be designed into a decentralised Metaverse to safeguard humans against violations of consent?

To address these research questions one of the main contributions of this paper is to provide an extended definition of the Metaverse.

Our methodology includes a literature review of definitions of the Metaverse. We review the risks and challenges of consent on Web 3.0 infrastructures. We design a framework for sharing agreements of consent, a Shared Consent Framework or "SCF". A SCF provides protection of human privacy, integrity and autonomy with technology infrastructures of the Metaverse. We perform a descriptive analysis of the XPRIZE Rapid Reskilling project, which uses Mixed Reality technology for training. Our analysis also demonstrates how the proposed shared consent framework could be applied. We propose an approach using AI bots such as ChatGPT that can be used to develop practical implementations of our shared consent framework. The paper finally reflects on the future of shared consent frameworks and alternative approaches that may protect users of the Metaverse against the risks and violations of consent.

2 What is the metaverse and implications for consent

Decentralisation, in the context of the Metaverse, is defined by how control and decision-making is transferred from a centralised body, such as an individual, organisation, or group, to a distributed matrix or network of resources or functions. A decentralised Metaverse is administered, managed and owned across a network of participants as opposed to being run by a single authority, for example, Meta Platforms Inc. Ownership in a decentralised Metaverse is established using blockchain technology and cryptographic keys to give individuals ownership over digital content. Decentralised autonomous organisations also known as "smart contracts" are emerging as ways of governing access and ownership of assets in a decentralised Metaverse. Smart contracts are self-executing and self-regulating. Powered by blockchain technology, they can execute predefined rules without the need for centralised authorities or other intermediaries. Decentralisation facilitates interoperability between virtual worlds, so that digital assets can be used and seamlessly move between virtual spaces.

A decentralised system aims to reduce the need for the trust that participants must have in each other and constrain their agency to enforce authority or control over each other in ways that do not undermine the integrity of functions and resources of the network. For the Metaverse, each individual user, or agent that interacts with it, must be able to manage their own agency whilst sustaining the agency of other users. For that there will be a need for decentralised hardware architectures, networks, and communications.

2.1 Origins of the term metaverse

Metaverse, a term first coined in science fiction, is a combination of the prefix "meta", meaning beyond, and "universe". It refers to shared virtual worlds where land, buildings, avatars and even names can be bought and sold, often using cryptocurrency. In these environments, people can meet up with friends, visit buildings, buy goods and services, and attend events.

Mystakidis refers to the Metaverse as "a post-reality universe, a perpetual and persistent multiuser environment merging physical reality with digital virtuality" (Madary and Metzinger, 2016; Mystakidis, 2022). He states further that it, "is based on technologies that enable multisensory interactions with virtual environments, digital objects, and people" (Mystakidis, 2022). Within the Metaverse and with regard to commerce, "consumers can engage with multiple tools that can be cocreated using real-time data ... that brings together a range of stakeholders to cocreate value" (Dwivedi et al., 2023). Anshari points out that businesses, "are

starting to use the Metaverse to expand their service network and establish new value co-creation for customers. However, businesses may need to carefully assess the ethical implications of their data collection and utilisation procedures for business sustainability" (Anshari et al., 2022). Although there is promise of value co-creation, this will need to have oversight through frameworks of mediation, moderation and regulation.

The concept of the Metaverse has advanced during the COVID-19 pandemic as lock-down measures and work-from-home policies pushed more people online for both business and pleasure. The term covers a wide variety of virtual realities, from workplace tools to games and community platforms.

Many of the new platforms are powered by distributed ledgers (i.e., blockchains), using cryptocurrency and non-fungible tokens (NFTs), allowing a new kind of decentralised digital asset to be built, owned, and monetised. The combination of the Metaverse with blockchain provides a feasible way of providing non-repudiable proofs-of-ownership as well as priming the Metaverse for decentralised operations. The complexity of these operations though might not be able to be handled by existing architectures and processes, so there will inevitably be a call to support functions through the use of Artificial Intelligence (AI) that could handle the massively parallel interactions that are native to such platforms, especially graphics functions that procedurally generate visual 3D content on demand.

As noted in the introduction, body scanning threatens personal privacy and sovereignty due to the ability to abuse deep-fake techniques to replicate a human being to near biometric accuracy. The advent of neural radiance fields (NeRF) technology means the time to produce an accurate three-dimensional model from two-dimensional photographs is greatly reduced. A way of mitigating this form of personal "bio-data hack" would be to ensure that your digital biometric likeness has been secured as either an NFT or via storage on IP file servers, thereby allowing you to prove ownership of a version of your digital self.

2.2 The Metaverse as a 3D model

Metaverse is a term originally established by Neal Stephenson in his novel, Snow Crash (Stephenson, 1992), in which he describes a virtual world that is ubiquitous within his imagined future, it has become an expression to describe stacks of Web 3.0 technologies focusing on human-centric experiential modalities. What does all that mean?

Our definition of the Metaverse, encapsulates the fundamental underlying core technology, infrastructure, potential implementations and how it is consumed. The Metaverse is more than just software and avatars, it is an entire shift in paradigm from the primary Web 2.0 centralised based system to that of Web 3.0 infrastructures. At the core of the Metaverse is decentralisation. It is a system of unfathomable numbers of creators, co-creators, infrastructures, and domains of authorities. However, it should be remembered that the Metaverse could operate on either Web 2.0 (centralised) or Web 3.0 (decentralised) infrastructures.

According to Mathew Ball, a venture capitalist and angel investor who has written a series of essays about the future and infrastructure of the Metaverse, "When these two technologies (internet and computing) first emerged, all interactions were primarily text-based (emails, messages, usernames, email addresses). Then they slowly became more media-based (photos, videos, livestreams). The next elevation of user interface and user experience is into 3D. Secondly, if we think of [a] mobile [phone] as placing a computer in our pocket and the internet being available at all times, think of the Metaverse as always being within a computer and inside the internet." (Ball, 2021).

TABLE 1 Metaverse a three-dimensional model (Smith et al., 2023).

	WEB 2.0	WEB 3.0
Communication	Interactive	Engaged/Invested
Information	Dynamic	Portable/Personal
Focus	Community	Individual
Personal	Blogs/Wikis	Livestreams
Content	Sharing	Curation
Interaction	Web Applications	Smart Applications
Search	Keywords/Tags	Context/Relevance
Metrics	Cost per Click	User Engagement
Advertising	Interactive	Behavioural
Research	Wikipedia	Semantic Web
Technologies	Flash/Java/XML	RDF/RDFS/OWL

Many professionals and experts are looking at the Metaverse as a three-dimensional model of the internet, a place where you and other people, represent themselves using infinitely customisable avatars, permitting a level of self-expression previously impossible. At its core the Metaverse can be viewed as a three-dimensional version of the internet, as represented in Table 1, that is seen as the next step in its evolution, ideally accessed through a single gateway. Search Engines will need to take into account more of the context and engineering that will need to be created for the Metaverse through procedural, on demand generation of content, especially that created by generative AI applications. A discipline for engineering context, Context Engineering, has been developed for exactly this purpose (Smith, 2016).

2.3 The decentralised metaverse defined

While the "Metaverse" is a complex and multifaceted concept that has its roots in science fiction, it is rapidly becoming a reality due to advancements in technology. Here's a definition that encapsulates its essence:

The Metaverse is a decentralised, shared virtual domain that arises from the symbiotic interaction of digitally enhanced physical and cyber realities. The extra, prior unrealised dimension, situated at the crossroads of AR, VR, and the Internet, can be explored via various hardware platforms such as smartphones, VR headsets, and AR spectacles.

The core concept of decentralisation at the heart of the Metaverse, signifies that it is not governed by a single entity.

Instead, it is a mutual creation where different individuals and entities contribute to its creation and maintenance. Blockchain technology plays a pivotal role, providing a secure, transparent, and indelible ledger. It enables the formulation of decentralised apps (DApps) and smart contracts, which promote interactions in the Metaverse and also support the development and exchange of digital entities like Non-Fungible Tokens (NFTs) (De Filippi and Hassan, 2016).

Primarily, devices boasting VR/AR technologies serve as portals into the Metaverse. With the advent of 5G and mobile tech advancements, these experiences are becoming increasingly immersive and attainable, thus setting the stage for the Metaverse's widespread acceptance.

One way to comprehend the Metaverse, seen as an advanced form of the Internet, is through the OSI (Open Systems Interconnection) model. Here's a hypothetical mapping of the Metaverse's technical infrastructure and technologies onto the OSI model's seven layers:

- Physical Layer: Includes the hardware that powers the Metaverse, such as VR/AR goggles, smartphones, computers, servers, and wired or wireless tech for data transmission.
- Data Link Layer: This layer manages data transfer between network nodes using technologies like Ethernet for wired connections and Wi-Fi or 5G for wireless connections.
- Network Layer: Manages data routing, which in the Metaverse could involve tech like IP for directing data packets to their destinations.
- Transport Layer: Ensures end-to-end communication and reliability using protocols like TCP for reliable data transmission or UDP for faster, but less reliable, data transmission.
- Session Layer: Supervises sessions between applications, involving protocols and tech for managing user sessions within and across various virtual environments in the Metaverse.
- Presentation Layer: Ensures data is in a useable format, potentially involving technologies for rendering 3D graphics, spatial audio, haptic feedback, and other sensory data in the Metaverse.
- Application Layer: Includes the VR/AR applications, games, social platforms, and other software that users interact with in the Metaverse. Also includes blockchain-based DApps and smart contracts enabling decentralised control and transactions within the Metaverse (Lubin, 2022).

However, the development of the Metaverse also brings a host of ethical and moral considerations:

- Privacy and Data Security: The Metaverse will collect significantly more personal datapoints, including biometric, behavioural, and psychometric data. This leads to concerns about how this data is stored, used, and protected (Nissenbaum, 2009; Raine and Anderson, 2019).
- Identity and Anonymity: The Metaverse will likely facilitate the increased creation of illegal digital avatars independent of a person's real-world identity, which could result in issues like harassment or cybercrime (Turkle, 2011).
- Digital Divide: The Metaverse could accentuate existing inequalities for those who cannot afford or access the requisite technology (Norris, 2001).
- Ownership and Control: Even though the Metaverse should be decentralised, large tech companies could still exert significant influence. Issues of digital ownership also need to be tackled.
- Content Moderation: Balancing content moderation needs with principles of freedom of expression and decentralisation will be a challenge in the Metaverse (Gillespie, 2018).
- Mental Health: Lengthy immersion in virtual environments could affect mental health, including potential addiction and the effects of blurring the line between virtual and real.
- Physical Health: The long-term effects of using VR/AR technology are not yet fully understood and require further research (Kim et al., 2017).

These are truly complex issues that demand continuous dialogue and collaboration among diverse and inclusive groups of technologists, ethicists, policymakers, and it is crucial that these conversations take place now, before it is too late, while the Metaverse is still in its formative stages.

2.4 Volumetric capture

Volumetric video will play a key role in content creation in the emerging Metaverse. It represents a joining of traditional linear workflows with interactive media like games and digital environments. As more industries adopt volumetric video, content creators will have the opportunity to add richer, more immersive elements, engaging the viewer in the experience. The benefits can be profound, but businesses, teams, and software must evolve to meet future demand.

Volumetric video capture technology is a technique that digitises a three-dimensional space, i.e., the volume of space, object, or environment in real-time using an array of cameras set around a target (see Figure 1). The captured object can be digitised and transferred to the web, mobile, or virtual worlds and viewed in 3D. What makes volumetric video so powerful is that the final product does not have a "directors view" meaning there is no set viewpoint and as a result it becomes a declarative space where the end-user can watch and interact with the footage from all angles, enhancing their experience and heightening their sense of immersion and engagement.

The difference between 360-degree video and volumetric video is the depth provided with volume. In a 360-degree video, users can only view the video from a single, constant depth. With volumetric video, the end-user can play the director and control how far in or out they want to explore the scene (Demir, 2021). Application areas including medicine and sports science benefit from the ability to move anywhere in the captured 3D model to specific monitor areas. Because of the potential precision of replication of content and context, volumetric video capture is a potential avenue of abuse and an attack surface for anyone wishing to subvert user privacy or identity. With the advent of phones with embedded drone cameras, such as those from manufacturer, Vivo, volumetric capture will be soon available with anyone who has a phone and even 3D motion

FIGURE 1
Depiction of volumetric capture from a studio.

capture is possible if users network their phones and associated drone devices. (Jurrien, 2021).

A company called [Anonymous-Version], is focussed on the development of autonomous intelligent markerless camera sync, volumetric capture software called SpatialScan3D. It is not only efficient and accurate but also respects user privacy via automatic facial anonymisation and all neural processing done on-device, ensuring that users are safeguarded from the analysis of their data by third-party services, protected by end-to-end post-quantum encryption.

3 Challenges of consent

The concept of consent is fundamental to the protection of individual privacy and the safeguarding of personal data. However, despite the existence of laws and regulations governing the collection, use, and storage of personal data, e.g., the European Union's General Data Protection Regulation, GDPR, many organisations and individuals continue to engage in practices that violate consent and compromise the privacy of individuals (GDPR and European Union, 2020; Koops, 2014). Several categories of actions that would violate consent are:

- Unauthorised data collection: One of the most common examples of violations of consent is the unauthorised collection of personal data. For instance, companies may collect data from individuals without their knowledge or consent, using cookies, browser tracking, and other data collection tools.
- Sharing of personal data without consent: Companies may also share personal data with third parties without the individual's consent. For example, Facebook was accused of sharing the personal data of its users with Cambridge Analytica, a political consulting firm, which used the data to target political advertisements during the 2016 US presidential election (Kleinman, 2018).
- Misuse of personal data: Another violation of consent is the misuse of personal data by organisations. For instance, companies may use personal data for purposes other than what it was collected for, such as for targeted advertising, even if the individual has not consented to this use.

Prior to defining challenges of consent in the Metaverse, we need to examine the meaning of the rights of privacy, integrity, and autonomy.

Privacy is associated with the right to protection of personal identity. European data protection laws provide definitions of personal identification rights. Often however, the concept of privacy is tied to personal integrity (validity and authenticity) and personal autonomy (management and control) over one's own data. This may include extending protection of our personal rights to control over our biological data and materials, including many forms of biometric data (e.g., heart rate, temperature, emotional data points through voice analysis, etc.). Some have argued that laws cannot provide this level of personal control and protection over personal data (Grawert, 2015). Even as early as 2003, the Australian Office of Federal Privacy had recognised the challenges presented by the ties between personal information privacy and personal bodily integrity, then stating (Australian Law Reform Commission ALRC and Australian Health Ethics Committee AHEC, 2003), ". An attempt to maintain a clear demarcation between different types of privacy protection may be problematic in light of new technologies which involve the merging of biology, mathematics and computer science, namely, biometrics and bioinformatics. Such developments give rise to new forms of body templates or records which further blur the distinction between personal information and its source in individual humans, rendering the concepts of information privacy and bodily privacy inherently interrelated." [3, p.280]

In developing Metaverse experiences a major concern will be privacy and general consent frameworks around extended reality, which includes virtual reality, mixed reality, and augmented reality. The Metaverse is a co-created experience, made up of multiple stakeholders, including autonomous individuals and other organised and commercial initiatives, that build value (economic or social). Zwass describes the nature of goods that dominate co-creation are often digital and non-rival, and that they are not easily excludable (Zwass, 2010). While there are potentially many beneficiaries of a co-created Metaverse, the stakeholders (e.g., a

firm developing the digital community, a sponsor or creator of digital content, or an individual "player") may not have the same access, perception, and analytical power over the use of data in the co-created digital space (Zwass, 2010).

Investigation into what data is collected through these Metaverse systems will be needed as well as where that data goes and how it is used. Collection of biometric and physiological data will generate intelligence on user neural activity and that will require "rights frameworks" to support ethical utilisation and exploitation. Kent Bye comments, "If we do not have mental privacy and biological privacy, some of the new technologies could essentially read our minds, model our identity, reach fine-grained and contextually relevant conclusions, and then nudge our behaviours to the point where it undermines our intentional actions. (Roettgers, 2021)." Problems could accelerate in the Metaverse primarily because of the layer of immersiveness that is inherent to the technology. New Metaverse oriented standards are being created by groups like the Khronos Group and Open XR with a strong focus on interoperable interfaces (Roettgers, 2021).

3.1 Unauthorised surveillance: a leading violation of consent

Protection of data security and privacy is a vast challenge for Web 2.0. Data breaches that are becoming increasingly common and can have significant financial, legal, and reputational consequences for organisations and the individuals affected by them. Many forms of social engineering exist, e.g., phishing, vishing, pretexting, baiting, water hole attack, scareware, etc. These are types of sophisticated methods of tricking individuals into divulging sensitive information. Such methods can be difficult to detect and prevent. It is important for individuals and organisations to be aware of these tactics and to take steps to protect themselves. Often organisations will have policies, procedures, and technology in place to detect and respond to data security threats. However, what is more alarming (because it is not always protected in societal laws as a violation of consent) are the cases of unauthorised surveillance.

Unauthorised surveillance refers to the act of monitoring or collecting information about individuals or organisations without their knowledge or consent. Here are a few examples of real-world instances of unauthorised surveillance:

- PRISM: In 2013, Edward Snowden leaked classified information revealing that the National Security Agency (NSA) had been conducting a secret surveillance program called PRISM, which collected data from major internet companies such as Google, Facebook, and Apple without the knowledge or consent of the companies or their users (Eggen, 2013; Greenfieldboyce, 2013; Greenwald and MacAskill, 2013).
- Stingray: Stingray is the brand name of an IMSI catcher, a surveillance device that mimics a cell phone tower and tricks nearby mobile phones into connecting to it. Stingray devices have been used by law enforcement agencies in the United States to track the location of individuals without their knowledge or consent (EFF and Electronic Frontier Foundation, 2017; Goldman, 2021; Silverman, 2015).
- CCTV: In some cases, the use of CCTV cameras in public spaces, such as in street, squares or shopping centres, can be considered as an unauthorised surveillance, especially if the cameras are not clearly marked or if the data collected is used for purposes other than those stated (BBC News, 2018; Hedger, 2019; Lassiter, 2017; Privacy International, 2020; Privacy and Human Rights Report, 2017; The Information Commissioner's Office, 2020).
- Phone and Internet surveillance: Some governments have been accused of conducting widespread surveillance of their citizens' phone and internet activities, without their knowledge or consent.
- Surveillance Capitalism: This refers to the way some companies collect and use data on users without their knowledge or consent, often for targeted advertising or other purposes.

These are just a few examples of the many instances of unauthorised surveillance that have occurred in recent years. Unauthorised surveillance can be a violation of individuals' privacy and civil liberties, and it is important for individuals and organisations to be aware of the potential risks and to take steps to protect themselves. With the addition of technology such as AI and Machine Learning algorithms, comes the extra abilities for facial recognition, movement recognition, big data analytics with data stores to predict and possibly promote individual behaviours. If metrics are gathered regarding mental or psychological state through algorithms or sensors in Metaverse portals or devices, then individual behaviours could also be collectively manipulated through social engineering to influence desired societal directions.

3.2 Violations of consent in the metaverse

The Metaverse, as represented in virtual worlds, is becoming increasingly popular, with millions of users creating digital avatars and engaging in virtual activities. However, the collection and use of personal data in the Metaverse can raise significant privacy concerns, as individuals may be unaware of how their personal data is being collected and used. For example, virtual reality (VR) headset manufacturers may collect data on the movements and interactions of users, which can be used for targeted advertising, market research, or even for psychological profiling. Additionally, virtual world providers may share personal data with third parties, such as advertisers or data brokers, without the individual's consent.

Metaverse interactions will inevitably not just be played out through VR or AR headsets but will utilise affordances of brainwave capture to optimise experiences. This will raise issues regarding the ethics of how that data is used as well as who can afford the technology. There are already technology "poverties" and "divides", especially regarding internet access (Aguh, 2018; Lores, 2021; United Nations, 2020). How will these translate into accessibility for the Metaverse?

In 2010 Tan Le's TED talk focused on how her company's technology could read brainwaves (Le, 2010). Could brainwave datasets be processed, through cumulative AI collation, to forecast our own potential thoughts and actions? If so, what precautions and constraints, as well as regulations will be required to protect user rights (Soepeno, 2021) ?

In 2008, Edward H. Spence proposed a framework for operating in a virtual world with morality and ethics that were grounded in a framework of shared consent (Spence, 2008). Spence proposed that as people adopt virtual avatars as identities in the Metaverse these characters can be viewed as virtual representations or modes of presentations of real people, so must be afforded the same rights as actual people as well as behave, comply, and act in alignment with the moral principles of real-world human beings. Spence establishes moral and ethical drivers for virtual worlds based on the work of Alan Gewirth and his argument for the Principle of Generic Consistency (PGC; Gewirth, 1978). PGC demonstrates that any person acting with a purpose, embodied as an avatar or agent in virtual spaces, has rights to freedom and wellbeing that are generic. This is the case as if the person was acting with purpose in the real world, they would have such rights and so by extension these rights should be maintained if they are acting with purpose in a virtual world. In legal frameworks corporations can be defined as an individual persona so this could lead to businesses having equivalent rights too when represented in virtual worlds.

According to the American Bar, "Interestingly, while the Court has concluded that corporations are "persons" within the meaning of the Equal Protection Clause of the 14th Amendment, the Court has been quite reticent to concede that corporations are "citizens" for the purpose of the Privileges and Immunities Clause." (Torres-Spelliscy, 2022).

Cathy Hackl, a futurist on AR and VR, in 2020 wrote for Forbes on the emerging Metaverse, also highlighting how tracking would happen of body movement, brainwaves, and physiological responses (Hackl, 2020). She expressed concern that privacy violations and data piracy would spill over from current 2D internet and mobile platforms into 3D virtual spaces where terms and conditions people might need to agree to might be even more extensive. As users so often gloss over such agreements, hastily agreeing to them, a question needs considering. What would be the consequences in expanded realities of virtual worlds associated with the Metaverse where complexity of interactions and datasets would be considerably more complex?

Kavya Pearlman is Founder and CEO of XR Safety Initiative, her organisation is trying to help build guidelines around privacy, ethics, and safety for the emerging realities. She has declared that organisations like hers must enable trust and help build safe, immersive ecosystems. (Hackl, 2020).

Identities, particularly in the form of digital avatars created by Artificial Intelligence Metaverse algorithms, may also cause disruption and moral dilemmas. In Metaverse interactions, particularly in video games, how would we treat AI-based realistic characters with almost human personalities and emotions? Bartle raises concerns over toxicity, or bad behaviour where players are harassing or bullying someone. There is a need for creators of Metaverse environments to make them safe spaces for everyone. As norms change, such as around sexuality, so must virtual affordances and types of moderation. (Bartle, 2004; Bartle et al., 2009; Bartle, 2020; Takahashi, 2021).

The Integrity and Autonomy needed for designing human experience can be architected through Fraga's take on Ontological Design. Ethics for the Metaverse, has come to be called Meta-Ethics as in the paper discussed earlier by Spence (Spence, 2008). Janko Roettgers in 2021 took this on in his article "How to Build A Safer, More Inclusive Metaverse" (Roettgers, 2021). Roettgers highlights how Tiffany Xingyu Wang, co-founder and president of the OASIS Consortium, is establishing processes for safety for emerging social platforms (Roettgers, 2021). In August 2021, OASIS relaunched as an industry consortium that promotes ethical standards and practices for the Metaverse. Wang indicated that over 40% of United States internet users have experienced online harassment. Current social platforms were built without safeguards with moderation added late in the process. The Metaverse is likely to attract questionable audiences without guardrails. A key issue of potential harassment may feel even more personal and threatening in life-like virtual environments. Safety will need to be a priority supported both by junior moderation staff as well through executive roles. Diversity will be critical in the safety workforce. Safety, privacy, and inclusion for the Metaverse will need to be established with a panel of experts that are diverse and inclusive. A major output will be a consensus document of shared standards in 2021 (Roettgers, 2021), one whose values are hoped to be adhered to by companies across the industry. This will be necessary to not repeat the lack of safety foresight seen in creation of previous platforms (Roettgers, 2021). In a July 2021 article, Benjamin Bertram Goldman highlights that the ethics of designing virtual worlds will lead to interactions that are more face-to-face and direct rather than impersonal and distant as seen in current social media channels (Virtual Reality Society, 2022). Reactions will be live and not asynchronous. Conflict is more likely so will need more effective forms of real-time moderation and regulation (Goldman, 2021).

A working example of a virtual Metaverse environment where the ramifications of consent, or more correctly the lack of consent frameworks adoption is leading to harassment, is the case of VRChat. One of the single most popular completely VR experiences available with over 7 million visitors per year, experiences multiple problems including virtual sexual harassment. With a female user population of only 18.43% this is a hugely male-dominated environment, this is reflected in the kinds of harassment being experienced (Maloney et al., 2021).

3.3 Enforcing ethical and moral standards in VRChat

The advent of Virtual Reality (VR) has ushered in a new era of social engagement, offering a platform for global users to interact in a seemingly tangible manner. VRChat is a prominent platform in this area and is one of the most widely-used social VR applications. However, the emergence of this novel form of social interaction has given rise to concerns about the enforcement of ethical and moral standards within such platforms. It is important to outline the exact issues that VRChat raises:

VRChat has recently been at the centre of several ethical dilemmas, primarily around user conduct. Reports of harassment, racial discrimination, and other forms of disrespectful behaviour have been common, posing substantial challenges to the harmony of the platform's community (Lombardo and Jones, 2021). The immersive quality of VR can amplify the impact of these experiences, potentially making them more damaging than similar interactions on traditional 2D platforms.

Another contentious issue is the normalisation of sexualised actions and content within VRChat. The platform's social norms often overlook age and gender considerations, leading to scenarios where physical intimacy is tacitly accepted without explicit prior consent. This raises serious concerns about the potential for exploitation and harm, particularly for younger users.

In response to these challenges, VRChat and other social VR platforms have initiated various measures to combat harassment and inappropriate behaviour. These include the ability to mute or block other users, report misconduct, and establish an invisible "bubble" of personal space to prevent other avatars from encroaching.

VRChat has also been striving to enhance its moderation system to better tackle these issues. However, the efficacy of these measures remains to be fully ascertained, and these measures may not be adequate enough to address the intricate and evolving challenges posed by the platform's rapid expansion.

The enforcement of ethical and moral standards in VRChat and similar platforms is a complex and ongoing endeavour. Despite the implementation of measures to combat harassment and inappropriate behaviour, these issues persist. It is evident that a comprehensive approach, combining effective moderation, user education, and robust safety features, is necessary to ensure a safe and respectful environment for all users.

Examples of violations within VRChat:

Example 1: One notable incident involved a user suffering a seizure whilst playing VRChat. Another player, utilising the username "Rogue13"noticed the situation and quickly cleared the area around the affected avatar, enforcing an impromptu personal space bubble. Other users also refrained from making loud noises or flashing lights, actions that could have exacerbated the situation. This example showcased an example of community-led enforcement of respect and empathy, in line with ethical and moral standards.

Example 2: Conversely, a well-documented case of harassment involved a VRChat user being persistently pursued by another player, who continually invaded her personal space and directed lewd gestures towards her. She repeatedly expressed her discomfort and requested him to stop, to no avail. Upon reporting the incident, the harassing user was promptly investigated and penalised, demonstrating VRChat's commitment to enforcing its community standards.

While technological advancements like VRChat offer unprecedented opportunities for interaction and creativity, they also open the door for new forms of misconduct. By actively refining and enforcing their community standards, equipping users with comfort settings, and leveraging a robust moderation system, VRChat exemplifies how platforms can maintain ethical and moral standards in virtual environments. However, as VR and other immersive technologies evolve, platforms will need to continuously adapt and refine their approaches to ensure a safe and enjoyable experience for all users.

3.4 Protections for addressing consent challenges in the metaverse

The Open Systems Interconnection (OSI) architecture of the Metaverse must be overseen in its layers by systems of consent that moderate everything from the foundational network hardware to the high-level applications such as browsers and other applications. As Metaverse architecture is emerging as a decentralised, serverless ecosystem it is critical that any consent frameworks also operate through similar protocols and processes to enable a balance between respecting data integrity and focusing on performance-oriented strategies.

Without regulation of consent in a decentralised manner the likelihood is that Metaverse experiences and applications will end up in walled gardens of the kind that Facebook and other social media platforms currently manage. However, decentralisation of systems and communities will be harder to regulate (VRChat Community Guidelines, 2023). In order to service decentralised resources and communities, it is inevitable that Artificial Intelligence support will be required. So Metaverse consent regulation cannot be seen in isolation but must work in unison with AI regulation. So, we propose that current calls for the regulation of AI should also be applied to the mediation of consent in Metaverse regulation.

The European Union's Artificial Intelligence (AI) Act mainly seeks to enhance regulations concerning data quality, transparency, human supervision, and accountability. Additionally, it strives to tackle ethical concerns and operational hurdles in diverse sectors, including healthcare, education, finance, and energy. The bedrock of the AI Act is a system of classification for levels of risk an AI technology to safety or human rights. The framework's four risk tiers of unacceptable, high, limited and minimal could also provide a basis for Metaverse risk classification and enforcement. The risk levels are outlined in Table 2.

At a minimum, Metaverse regulation needs to provide cover for data quality, transparency, human supervision, and accountability. These efforts must centre on ethical concerns, rights, safety and operational hurdles, initially for specific sectors. Compliance for additional laws will not just have to be in alignment with the EU AI Act but associated acts of law such as the EU's Digital Services Act and Digital Markets Act. From 8 December 2024 the EU's Product Liability Directive provided redress for those having experienced liabilities arising from AI use. With the Directive, AI's can be considered "defective by default" if their operation is too complex to be explainable. The EU AI Act will start to be formally enforced, especially around prohibited uses of AI, from February 2025.

The Consent framework in this paper proposes enforcement through a decentralised Metaverse, coupled to Artificial Intelligence extensions and processes, for which oversight is provided for through a common integrated architecture. A provisional Shared Consent Framework is highlighted in Figure 2.

The five stages in Figure 2 need to have Ethical Data Oversight, Management and Deployment. The stages need to be overseen by a Shared Consent Framework that manages every data handling point or process that centre on sequential stages of (i) Data Capture and Generation, (ii) Packaging and Categorisation as well as (iii) Servicing and Exploitation. The framework polices and authorises data permissions, access, and utilisation.

The application process of the SCF is illustrated in Figure 2. This begins when User's Metaverse activity and biometric data is captured via an XR headset's sensors. The data is digitally packaged to generate a Digital Identity Dataset that can be utilised for enhanced empowering experiences or be exploited for manipulated experiences or controlled commercial gains. It is critical for the success of this framework, that all processes and data should be only stored locally on a user's device but vitally, if applications are allocated consent, selective data could then be

TABLE 2 AI/metaverse risks (EU and The Aritificial Intelligence Act, 2023; EU and European Commission, 2023; World Economic Forum, 2023).

Tier	Risk
Minimal	*Allowed to be used with little requirements other than transparency obligations.* Examples: • Spam filters • Video Games
Limited	*Not explicitly banned or listed as high-risk, largely left unregulated such as Chatbots*
High	*Permitted, but developers and users must adhere to regulations that require rigorous testing, proper documentation of data quality and an accountability framework that details human oversight. Subject to specific legal requirements.* Examples: • critical infrastructures (e.g., transport), that could put the life and health of citizens at risk • educational or vocational training, that may determine the access to education and professional course of someone's life (e.g., scoring of exams) • safety components of products (e.g., AI application in robot-assisted surgery) • employment, management of workers and access to self-employment (e.g., CV-sorting software for recruitment procedures)
Unacceptable	*A clear threat to the safety, livelihoods and rights of people. Systems will be banned with little exception that:* • Employ subliminal, manipulative, or deceptive methods to skew behaviour • Prey on the weaknesses of individual people or certain groups • Use Biometric classification systems predicated on sensitive attributes or features • Conduct Operations for formulating social scores or assessing reliability • Engage in risk evaluations to predict criminal or administrative violations • Generate or broaden facial recognition databases via non-specific scraping • Deduce emotional states in contexts such as law enforcement, border control, workplaces, and schools

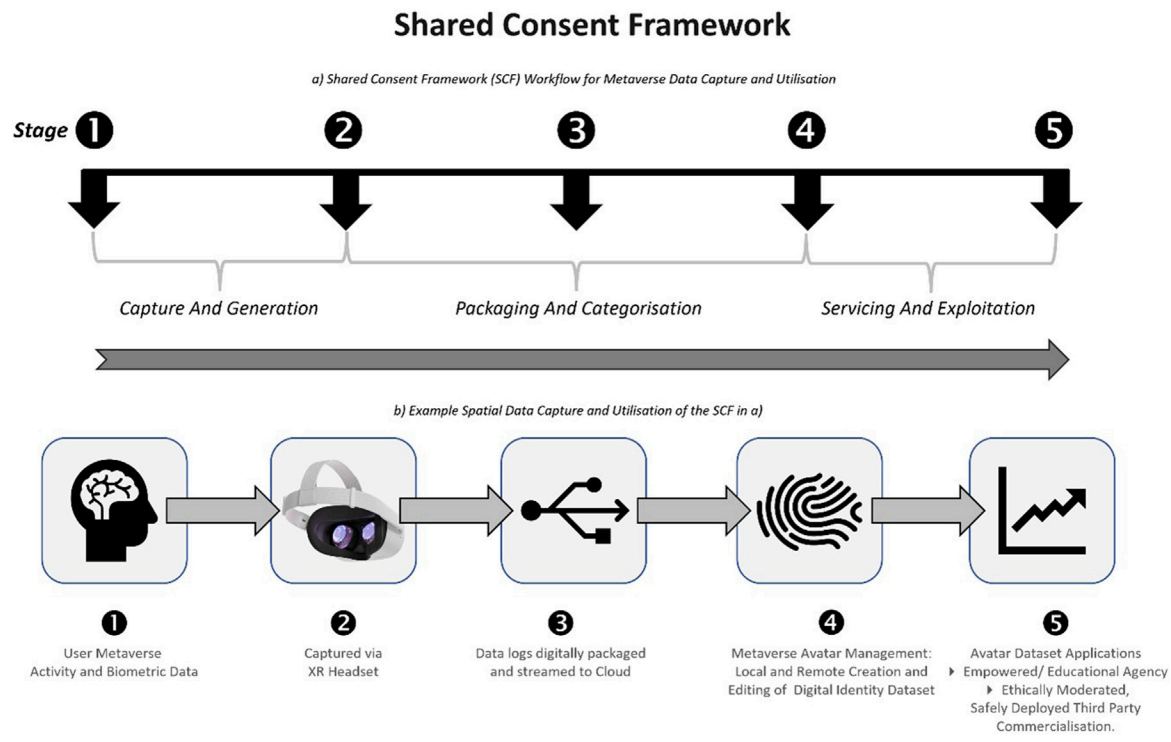

FIGURE 2
Consent framework: **(A)** Workflow for metaverse data capture and utilisation **(B)** example spatial data capture and utilisation in the shared consent framework (SCF) (Smith et al., 2023).

shared beyond the device, something that is explored later in this paper in Section 7, "Discussion: Implications for the Consent Process". In the next section we describe the XPRIZE "Rapid Employment Accessibility Platform (REAP) (REAP Technologies, 2021). The REAP platform design aligns with the five phases and supports the underlying principles of the Shared Consent Framework. It is a testing of the SCF within the limited scope of the XPRIZE project.

4 Experiences with the XPRIZE rapid Re-skilling competition as seen through the lens of the shared consent framework (SCF)

XPRIZE, a $5 million Rapid Re-skilling Competition, is based in the United States (XPRIZE, 2021). XPRIZE is a non-profit organisation that produces multiple innovative competitions that

are designed to solve the world's greatest challenges. In this case example we consider challenges of consent and explore possibilities for better engagement with safeguards in the Metaverse. We reflect on the authors semi-final entry solution in the XPRIZE Rapid Re-skilling Competition the "Rapid Employment Accessibility Platform" (REAP) (REAP Technologies, 2021). The REAP solution helps protect long-term employment for vulnerable workers through Mixed Reality training.

The XPRIZE REAP team leader explained, "Now more than ever, we need reliable ways of upskilling the whole of society, by taking full advantage of the latest learning technologies. We are incredibly proud of the fascinating work that our community is doing to empower those vulnerable to job loss."

4.1 REAP technologies and platforms

XPRIZE Rapid Re-skilling challenges teams to create effective rapid training and re-skilling options for people who are most likely to face unemployment in the United States. The aim of the competition is to reduce training time by at least 50% and will provide this training to jobseekers for free.

The REAP team consists of Kryotech, Maaind and Ravensbourne University London. The consortium developed a Neuro-Adaptive Mixed Reality Training platform in order to place 350 participants into full-time jobs. The REAP Multi-disciplinary Training environment has AR/VR elements that are mixed with live training, of, for example, "machinist in an auto-repair industry" or "operation of CNC machines and lathes" (XPRIZE, 2021).

A typical use case, of how an XPRIZE "customer" goes through the Rapid Reskilling experience begins by assessing experience of a user of virtual training through a voice analysis app on their mobile phone. This establishes what state they are in emotionally and then can suggest guidelines to optimise how they are for improved learning, a flow of guidance that is explored more in the next section.

4.2 Validating SCF: an example through REAP addressing challenges of consent

Within the XPRIZE Foundation Rapid Reskilling project (that three of the authors of this paper have led in delivering) it was found that biometrics were notoriously difficult to monitor in industrial environments within which participants were to be upskilled (Newell, 2019; Di Manno, 2021). As a result, voice stress analysis was chosen as a profiling tool, and associated machine learning utilised to determine a psychological state mix of up to 32 different datapoint emotions that could be transformed, guided, or channelled for enhanced learning and skill practice. Having any kind of data or algorithm that frames content created by users, like voice responses, requires appropriate securing of permissions to qualify a right to process the content as well as to how it will be stored, shared, made accessible or destroyed. These permissions cannot be small print in terms and conditions or privacy policies of vendors.

The design of the REAP Platform is a form of validation of the SCF in that it supports the principle that ownership must not be implicitly transferred or utilised without explicit consciousness, awareness and understanding informing the users agency and authority to share their personally generated data assets. *A priori* awareness and contract must be accompanied with regular assessment of consequences of use.

In the case of XPRIZE participants this authority was contracted and clearly registered with participants at the onset of them getting an account to access training services on the project mobile app. Voice analysis was utilised for profiling and to refine the delivery of the training. As the data generated was being collaboratively harnessed and channelled in a bespoke personalised way with training participants the opportunity for abuse or risk of ethical violations around its use was regularly tracked and overseen by the participants as well as stakeholders delivering the programme.

One of the biggest issues with the Metaverse is the need for end-to-end encryption in order to protect body image and biometrics. Kryotech's post-quantum encryption algorithms technology was brought into the REAP Platform solution to ensure end-to-end encryption of the voice data as collected through the mobile app. Kryotech specialises in advanced cyber security solutions for the edge of computational innovation. Kryotech are a company based around an ethical framework of humanity and ecology before profit. They are passionate about securing their future in the Metaverse by ensuring that we own our virtual identities now and forever. As humanity adopts the Metaverse ensuring that our personal identities, avatars, and data are secured and protected with post-quantum encryption becomes paramount. Kryotech is passionate about ensuring that our data and digital selves remain our own.

The REAP trainees were exposed to learning materials that adapted to their analysed vocal inputs. Learning materials were delivered across desktop, mobile and virtual platforms to provide access to as many users as possible of varying levels of technological skill and access. By deploying these novel mechanisms for training machinists, REAP were able to demonstrate increased knowledge retention and absorption in users of the platform during the testing period. Feedback tuned real-time learning is not easily achieved outside of a Metaverse environment due to the varying nature of everyone's capabilities. Therefore, by leveraging Metaverse technologies REAP were able to provide equitable access to learning and upskilling without disparity between users of different socio-economic backgrounds. The experiences also informed soft-skill development for employability and self-empowerment of participants as well as guided the facilitation of collaboration practices and dynamics when doing group immersive activities. This allowed the tutors to become informed of the ethical adjustments that were needed for individual challenges and the collective dynamics of the group. This was noticed when teaching participants migrating from individual collaboration literacy development to group collaboration literacy.

In terms of biometrics, the trainees Metaverse activity and biometric data is captured via the Mixed Reality headset's sensors. The data is then digitally packaged to generate a "Digital Identity Dataset".

This case example can be assessed in stages as seen through the lens of the Shared Consent Framework previously presented in Figure 2. The XPRIZE REAP version of the framework and flow of experience is outlined in five stages.

The first stage of the process for taking a participant through Machinist training involves getting permissions and authorisations to capture the user's biometric voice data.

Once authorisation has been obtained the participant is taken through the second stage of capturing voice data through the sensors of an XR Device, Mobile or Laptop.

A third stage ensures the data gathered related to the voice recordings and logs is packaged into a dataset related to the person's identity and streamed to the XPRIZE Cloud storage in a way that can be monitored and overseen by the participant or user.

A fourth stage running alongside the third stage ensures all processes related to user data capture and transportation are encrypted, end to end using post-quantum encryption of identity data. The raw data is then processed to extract salient features such as emotional state and focus.

The extracted features are then collated in a final fifth stage to generate the VR and AR app and in person guidance that will improve focus, learning as well as self-confidence, a delivery stage prescient of future production to be done in Metaverse environments.

This is achieved alongside the practice of machining skills to provide enhanced precision and exercise of skill. In addition, the features observed are utilised to enrich personal development and group collaboration.

Rights of consent were protected throughout by ensuring users had oversight of data gathered, its processing and its sharing. Prior authorisations determined the level of privacy while encryption and user moderation ensured autonomous access. With all this monitoring in place, integrity of data collected and shared, as well as of participant identity was ensured.

These five stages reflect a shared consent process that mirrors what will need to be enshrined in Metaverse related journeys curated via biometrics and encrypted data management to enhance application engagement, experiences, education, and accountable outcomes.

Metaverse experiences, like many existing AR and VR curated experiences, are likely to be experienced at first individually but social elements will inevitably make the experiences more interactive as well as more collaborative. It may appear that ethical oversight for Metaverse technologies is difficult to enforce at the individual level but that is the priority. When individual oversight is effective then group and community oversight will have more integrity and sustainability (Chouhan et al., 2019).

5 Limitations of existing consent frameworks

Frameworks that were originally regulation structures, such a GDPR and the United States's California Consumer Privacy Act (CCPA), have since become falsely interpreted as Consent Frameworks.

CCPA is privacy legislation that was enacted in 2020 and applies to private sector businesses that collect data about residents in the United States State of California only. The consumers have the rights to know when personal information is being collected about them, to delete such information, to opt-out or prevent the sale of such information to third parties, to be treated with non-discrimination (e.g., no discriminatory pricing), right to correct and right to limit. Although the consumers have these rights, the businesses are under no obligation to obtain consent from the consumers. For example, businesses have to notify that they are collecting cookies, but do not have to receive permission from consumers to begin doing so. (State of California and USA, 2024; Cloudfare Inc, 2022). CCPA legislation is implemented through a central governance approach, but falls short of being a consent framework.

For clarity the GDPR website states, "Contrary to popular belief, the EU GDPR (General Data Protection Regulation) does not require businesses to obtain consent from people before using their personal information for business purposes. Rather, consent is just one of the six legal bases outlined in Article 6 of the GDPR. Businesses must identify the legal basis for their data processing." (Wolford, 2022; EU, 2024) The five other lawful basis when a business does not need to seek consent are: (1) if a business has a contract with an individual to supply services and it is part of fulfilling that contract, (2) compliance with processing data for a legal obligation, (3) for vital interests, for example, the data processing could protect a life, (4) to complete a public task performed by a public authority, (5) legitimate interests that could include commercial benefits for a private organisation (as long as the act does not affect the individual's rights and freedoms.) (Irwin, 2024).

This implies that so long as the legal basis for data processing is stated consent does not need to be obtained. Of course, such a basis is often buried in small print in the Terms and Conditions users agree to, so there is consent by default that must be agreed to indirectly through accepting the terms and conditions. This is a loophole and exactly the kind of example that demonstrates why existing frameworks such as EU GDPR fall short, and further calls for establishing a utility through which a consent framework can be implemented.

There is also the need for a digital "airlock" that isolates the user from the dangers of giving consent by proxy through accepting the legal basis of processing data that is embedded in the Terms and Conditions, an action often performed without even rudimentary scrutiny of the text. Although a choice is made, the consent is given without sufficient review of its basis, as such this is not informed consent–a practice that Google have been fined for by authorities in France where French data protection authorities said the company's version of obtaining consent was neither "informed" nor "unambiguous" and "specific." (Pearson, 2019).

6 Towards the implementation of a shared consent framework

In order for future projects in the Metaverse to benefit from a practical implementation of the Shared Consent Framework, we propose the following approach. The prior example case of the XPRIZE demonstrates that a SCF must go beyond existing approaches of regulations and facilitate effective consent through a process that is at least, informed, unambiguous and specific. We propose the following approach to achieve a practical implementation of a consent framework by using AI bots such as ChatGPT.

10.3389/frvir.2025.1401073

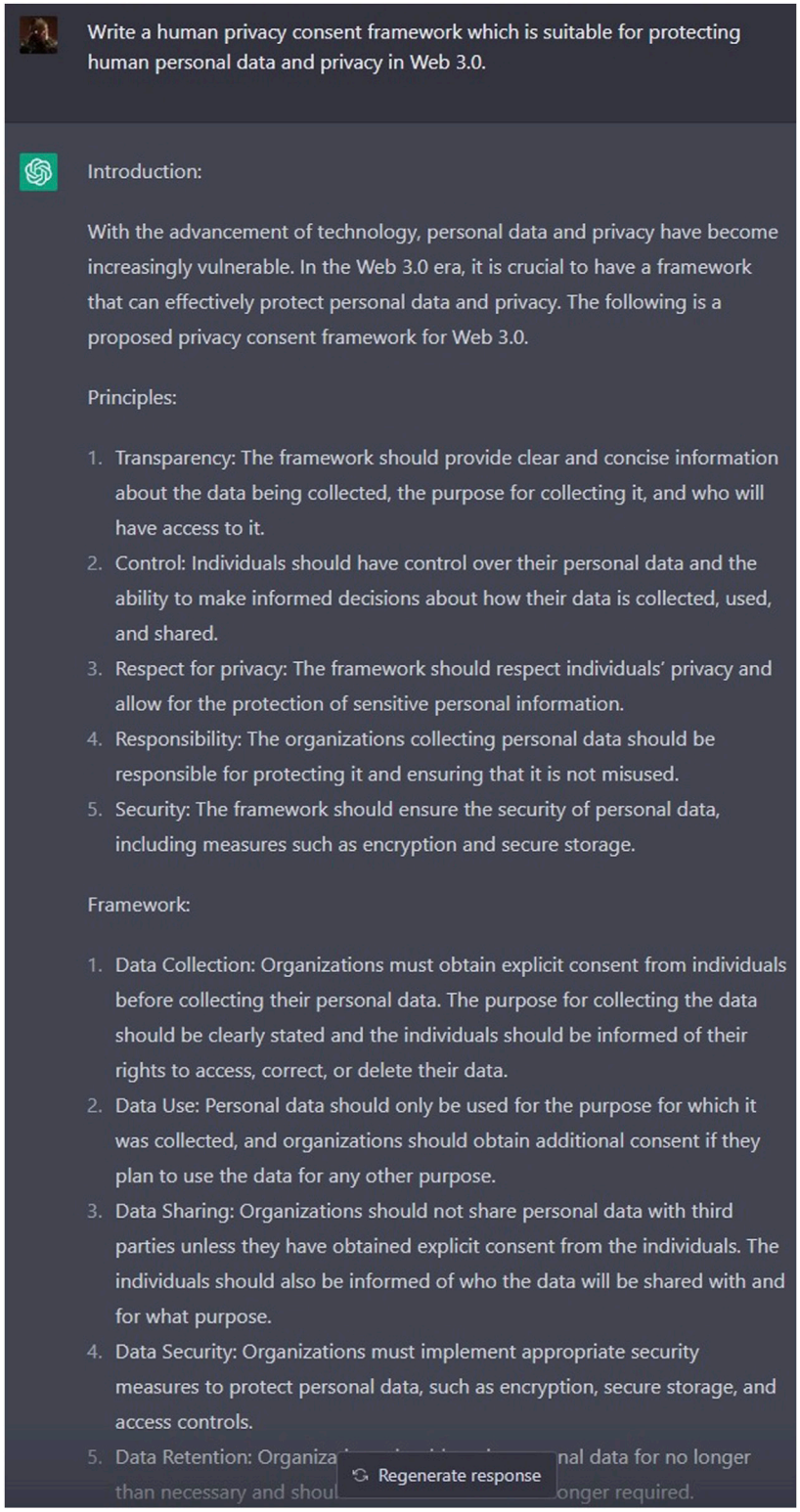

FIGURE 3
Attempt by ChatGPT to create an implementation of SCF suitable for Web 3.0.

With the advent of AI bots such as ChatGPT it would be possible to feed such Terms and Conditions into an AI that would provide such an informed, unambiguous and specific presentation and suggest to what terms could be consented. An author of this paper has produced software that allows you to upload a Terms and Conditions, or other policies, to memory and ask ChatGPT questions about the document. Additionally, it permits the exporting and saving of results. Through the right framing

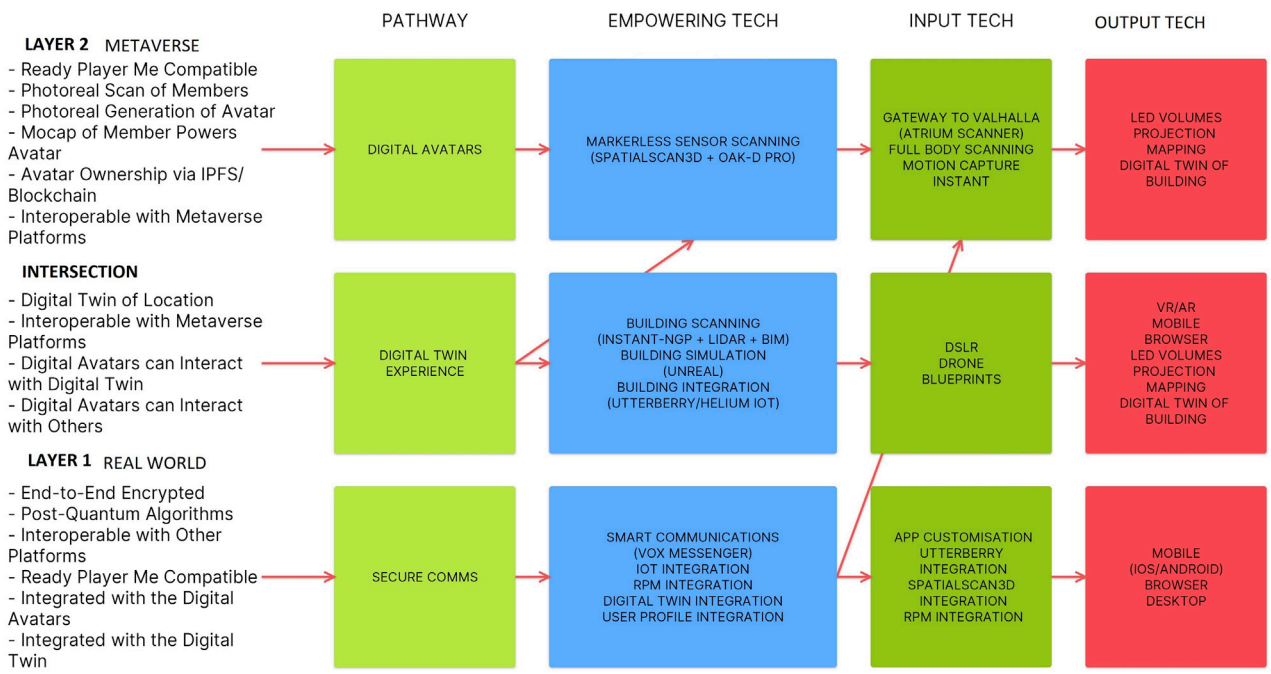

FIGURE 4
The four pillars of the digital self.

question ChatGPT could then provide such a summary that is informed, unambiguous and specific. This could form the basis of an automatically generated consent framework, as depicted in Figure 3.

With enough datasets of Terms and Conditions texts it would be possible to intelligently create a Consent Framework "on demand" that is bespoke to the individual and to the party requesting consent.

7 Discussion: implications for the consent process

A practical implementation of the Shared Consent Framework would have implications for the ways humans interact with their digital selves and infrastructures of the Metaverse. The major components of Metaverse architecture such as Web 3.0, Avatars, Experiences and Secure Comms (see Figure 4) would need to have the consent utility with the dynamically created consent framework embedded as a module within them. The Consent process should interface with the Input, Processing and Output stages of any data pathway through Metaverse space.

Figure 4 presents the model, the Four Pillars of the Digital Self, devised by (Webb-Benjamin). The model demonstrates the intersections of user interactions (pathway) with empowering technologies (power: empowering technologies including hardware, and software) through input and output technologies. With reference to the consent process (and the SCF, see Figure 2), the pathways of the Consent Utility would be activated prior to the Input Tech (SCF: capture and generation), between the Input Tech and Output Tech where processing (SCF: packaging and categorisation) would be carried out, and lastly just prior to content being displayed and outputted (SCF: servicing and exploitation).

A user's pathway is indicative of the entry point to a desired experiential destination or display output. The pathway of secure communications is a necessary base for the journey across experiences that a user's digital self may take. We use the terms "Layer 1"and "Layer 2"to differentiate between the real-world and virtual world or Metaverse. This semantically and actually matches the symbolic link between real-world and virtual world via digital twinning and digital avatars. In summary, Figure 4 illustrates how the digital avatar (persona) and the digital twin (environment) intersect. Given that all reality is subjective, the layer 2 reality (virtual) is effectively underpinned by the "real" foundations of layer 1 reality (the real world).

7.1 Potential for real-world applications of SCF

SCF could be implemented for public sector applications, where formerly mentioned legislative frameworks do not exist or do not offer guidance for public authorities. For example, since COVID there has been growing examples of higher educational institutions that offer courses as hybrid and digital offerings. While students have benefited from digital services such as recorded lectures, and online materials, some students have experienced the courses as challenging, especially in the case where a subset of students attend in-class while others access the same course through digital attendance. Educational institutions may seek to better understand the emotional experiences of the students, and to understand what criteria in the learning environment are needed

for a positive learning experience. To do this an application could be designed in some ways similar to XPRIZE REAP Platform, by implementing the SCF framework in the app design. Students could be offered to participate in a "welfare assessment exercise" and offered a SCF designed app to download. The app would facilitate them keeping a voice diary of their impressions of different learning experiences (SCF: capture and generation). This could be, for example, to record short impressions after attending a lecture face-to-face only offered course, or after attending f2f or virtually attend a hybrid offered course, or after attending a lecture virtually in a digital only offered course. The app could offer students summary feedback of their voice recordings based on an array of different emotional and psychological criteria (while respecting clauses to prevent risks or liabilities emerging from emotional inference or detection, referenced in the EU AI Act, identifying states of alertness or arousal rather than specific feelings or emotions). In other words, the SCF can be applied but in ways that are congruent with the EU AI Act. The recordings would be encrypted prior to saving sound segments on the student's phone (SCF: packaging and categorisation). The students could be asked to volunteer to share their data for analysis of group responses within a course. These types of assessments can be applied to many learning context (e.g., lectures, group work, practical exercises) (SCF: servicing and exploitation). Individual students could benefit by gaining understanding about which learning environments function best for themselves. Institutions could benefit by gaining understanding as to which learning context can invoke target group (e.g., bachelor students in engineering) positive or negative emotional responses.

Potential pitfalls or criticisms of the SCF can be directed at how well a designed application is able to implement the basic principles. Implementations would need to address technical, governance and organisational challenges. Technical challenges include how to address, for example, security in blockchain solutions. Solutions must maintain the protection of privacy versus perhaps business demands for transparency and auditability. Scalability (number of transactions) and functionality become an issue in cases of large, decentralised networks. Governance challenges include the need for acceptance of a new governance model (management of contracts, user participation in governance process) that may not mesh well with existing government legal and regulatory systems (e.g., personal identification, preventing embezzlement, fraud protection). Implementations can have organisational challenges that can impact user perception of openness, trust, willingness to adopt, and sustainability (some blockchain systems use a lot of energy).

7.2 Protocols for implementing the shared consent framework

To apply the SCF in real-world scenarios, ethically guided protocols need to be deployed for safe yet innovative implementation.

Ethical oversight of protocols must be grounded in affordances that allow for management of,

- *Transparency* of how the SCF will be deployed
- *Privacy* of the SCF mediated experience and the data artifacts that emerge from it
- Methods for ensuring resources and assets generated through SCF mediated experienced have their *Integrity* sustained and maintained
- Provision of interfaces and processes for the SCF experience that facilitate *Autonomy* for access and agency with gathered, processed and generated data, information, knowledge and intelligence.

Examples of how each of these affordances can be implemented and replicated will now be outlined.

7.2.1 *Transparency* of a SCF mediated experience

Transparency ensures that users find it easy to understand what, how and why data is gathered, utilised, and analysed at each stage of their experiential journey.

- Visual dashboards can provide users with real-time summaries of what data is collected, and by who, as well as the purpose for which it was gathered. For example, in a virtual environment, the parts that gather the most data could be shown in a heatmap.
- If biometric data is to be collected in VR systems, digital switches or toggles could be part of their interfaces to allow for data collection or to prevent it.
- The use of technology, such as AI, can be communicated through layers of explainability. As an example, in a job interview, conducted through an AI driven platform, explanations can be provided to the candidate for why they might have been shortlisted or rejected, with transparency on the criteria influencing the decision along with the priority, ranking or weights of importance of those criteria in the decision-making process.
- Records of consent obtained could be encoded in blockchain based immutable logs to ensure consent history is archived in tamper proof ways and records. Users will be able to audit how their consent was secured across systems at different stages of interaction.
- Just as packaged food has labels categorising nutrition levels, for Metaverse or Web 3.0 applications there could be standardised labels that disclose the data they collect (such as that gathered from biometrics or geolocation) as well as the uses the systems intend to put the data to (such as personalisation and customisation or research purposes)

7.2.2 *Privacy* of a SCF mediated experience

Securing privacy is important to ensure the user's data is safeguarded and that it is kept confidential during the user's interactions with the system as well as after exiting it.

- Authentication of users can be validated without storage of data or user details. Without revealing actual data, users can be allowed to verify their identity or credentials. For example, in using the Metaverse, an age eligibility check can be done without reference to date of birth that is stored or that requires specific access permissions.
- Decentralised AI Datasets can be used to train AI models without keeping sensitive user data in a centralised store. As an example, data on a user's local device can be used by AI

Personal Assistants rather than referencing or sending data to a repository on a central or remote server.
- Privacy can be preserved through encryption. All interactions in immersive Metaverse activities can be quarantined in end-to-end encryption. Any Data assets or artifacts recorded in Metaverse interactions, such as user gesture records, can be stored in encrypted formats only accessible to authorised entities.
- Minimal, required data should be collected for specific features. Consider a virtual retail store in the Metaverse. It can readily collect preferences for browsing. However, unless a purchase is about to take place, there is no need to gather personally identifiable information.

7.2.3 *Integrity* of the SCF experience

Fostering data integrity ensures that the resources, assets and information gathered through AI and Metaverse experiences mediated through the SCF, are managed for reliability, accountable authenticity, as well as ethical oversight and compliance.

- Use blockchain to validate and verify assets in the Metaverse, especially their origin and ownership, for assets such as NFT's. For example, an NFT artwork could have its full history provided by a system to include the NFT's creator, its previous owners as well as any modifications that may have taken place since its creation.
- Mechanisms for detecting tampering of asset integrity can be encoded through cryptographic signatures. This will ensure that there is no alteration of data and resources. As an example, summaries generated by AI could be tagged with cryptographic watermarks or hashes, ensuring that any unauthorised changes can be detected as well as provide evidence of AI generated content.
- Standards to independently and ethically certify the integrity of AI algorithms or Metaverse ecosystems can be done through regular audits by third party service providers. For example, an AI augmented video game selling virtual goods for enhanced in-game experience, can be certified as being fair in its pricing for different regions and users.
- Interfaces can be architected for reporting Incidents. If there is a breach of data security or there are concerns about unethical platform activity, alerts can be triggered to generate notifications to bodies or authorities that handle moderation, compliance or oversight.

7.2.4 Facilitating *autonomy* for SCF experiences

Autonomy ensures users can be empowered by providing them with control over their data, decisions, and actions within the AI or Metaverse systems they use.

- Users can control the management of their own identity across systems and platforms. Functions can be provided to enable users to have ownership as well as control over their identity across the platforms and systems they use. For example, when a user wants to log into a diversity of Metaverse environments they can do so using a digital wallet that operates through a decentralised network. Through that affordance they can have full freedom over which attributes of their identity are shared, depending on the Metaverse spaces they interact with.
- Consent can be managed through levels of granularity. Users can be allowed to modify their consent on the fly. For instance, during sensitive moments in VR facilitated meditation experiences, a user can switch data collection on or off.
- Frameworks can be provided for ensuring freedom of Data Portability and Transferability. These can help users to export their data in formats that play well with other systems and platforms. As an example, a user could transfer their personal profile, generated by AI, from one Metaverse space to another, without having to enter their preferences all over again.
- Collaborative User/AI decision making can be facilitated by allowing users to have the freedom to influence how AI recommendations are applied. For instance, if a user has better local knowledge while driving in a smart city environment, they might override route recommendations provided by an AI or Metaverse application.

7.2.5 Integrating SCF protocols across stages and domains

For SCF to be effectively integrated into a systems or platforms operations, any implemented protocols will have to,

- Be embedded into the lifecycle of design for systems, specifically through stages of ideation, development and deployment as well as the decommissioning of the systems or platforms.
- Ensure monitoring systems for ethics compliance can gauge alignment dynamically with laws such as the EU AI Act and its Product Liability Directive.

By combining any protocols with legal and ethical oversight mechanisms, the SCF can ensure that ethical protocol factors such as Transparency, Privacy, Integrity, and Autonomy are complied with across the diversity of AI, Metaverse, and Web 3.0 processes and environments that users might find themselves immersed in. These processes need to be deployed in ways that are informed, where the deployer does not just provide awareness or understanding for users but ensures that they register with the user, that the user demonstrates evidence of having gained awareness and understanding of their unfolding data journey. This needs to be done in an unambiguous way with specific references to activities that will be engaged with. Respect, accountability and enacted responsibility for such caveats will ensure risks and liabilities can be minimised in their effects. This will ensure users are not just notified of intended activities but also formally consent to them being carried out.

8 Reflections, concluding remarks and future work

In this paper we have explored and reviewed some key risks and challenges of consent and the knowledge gap in society that needs to be addressed to ensure that users of the emerging decentralised regulated (Web 3.0) Metaverse will have a fair and just use of the data that is generated within the Metaverse. We introduced a Shared

Consent Framework (SCF) and have reviewed how future case studies can be examined through the lens of that framework. We presented the challenges of consent within the project XPRIZE Rapid Reskilling, REAP project. We reviewed how current consent frameworks, such as the EU GDPR framework fail to address challenges of consent. An applied consent framework must be able to function in the decentralised Metaverse. We then proposed how AI tools such as ChatGPT could be applied towards the implementation of a consent framework that is informed, unambiguous and specific.

In future research we are looking to apply our Shared Consent Framework to other contexts, such as protecting the privacy, integrity and autonomy rights of workers, using advanced technologies in the workplace. For example, a study by Cadieux (Cadieux et al., 2021) has found that advanced technologies such as artificial intelligence and websites that misinform clients contribute to levels of insecurity and to the technostress process making them potentially harmful to the individual's health. We will also explore how the Shared Consent Framework could play a mitigating role in reducing stress caused by such technologies (Cadieux et al., 2021). Future research will further explore ethical issues in the emergent design of the Metaverse, such as the challenge of how to deal with the ownership of our digital data, and with that, the underlying ethical rights of transparency, privacy, integrity, and autonomy in a way that is informed, unambiguous and specific (Molka-Danielsen et al., 2021; Smith et al., 2020).

The Metaverse promises to be one of the biggest employers of the future. We need to ensure that we do not make the same mistakes that we did when we built the 2D internet. Facebook knows us in 2D better than our parents know us, but as we move into 3D version of Facebook then Meta could be one of many platforms that know us better than we know ourselves and be able to predict what we do next. How can an open Metaverse counteract such an affront? How can we educate ourselves in our own contexts as to what the Metaverse means? What does it mean to our businesses? What does it mean for our relationships, our identities, and the human condition? Further research should seek to answer these questions, to protect our ethical rights of transparency, privacy, integrity, and autonomy while still fostering user agency through experiences that are empowering, educational and entertaining, all within a decentralised Metaverse ecosystem.

In summary, this paper demonstrates the current gaps in existing consent frameworks which struggle to stifle violations of personal privacy and exploitation of our digital selves. However, until full homomorphic encryption (FHE) becomes consumer ready and adoptable, consent frameworks will become an increasing requirement for safe usage of the Metaverse. FHE, allows data to be handled and processed or "worked on" without requiring decryption at any point (Zama, 2023). For example, if you were to use ChatGPT, end-to-end full homomorphic encrypted, neither OpenAI nor, the LLM would see your data in an insecure, plain-readable format. In fact, no one does at present. Homomorphic encryption is the next-generation evolution of post-quantum encryption, or lattice-based cryptography (Zama, 2023). Once homomorphic encryption becomes the consumer mainstream there will be no need for consent frameworks, however, until then, we need to design and use frameworks as we have documented in this paper.

Data availability statement

The original contributions presented in the study are included in the article/supplementary material, further inquiries can be directed to the corresponding authors.

Author contributions

CS: Conceptualization, Methodology, Writing–original draft, Writing–review and editing. JM-D: Conceptualization, Methodology, Writing–original draft, Writing–review and editing. J-BW-B: Visualization, Writing–review and editing. JR: Methodology, Visualization, Writing–review and editing.

Funding

The author(s) declare that no financial support was received for the research, authorship, and/or publication of this article.

Acknowledgments

This paper is an original and significant expansion of the original concepts and ideas of the co-authors that were presented by the co-authors and listed in the Proceeding of the 56th Hawaii Int. Conf. on System Sciences (Smith et al., 2023). ChatGPT was used to create Figure 3 for demonstrative purposes. Model: 4o, Source: OpenAI, Version: 4

Conflict of interest

Authors J-BW was employed by Djinn Technologies Ltd.

Author JR was employed by Energy Diamond Consultancy Ltd.

The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

References

Aguh, C. (2018). How the "digital divide" is holding the U.S. economy back. *Venture Beat, Febr.* 10. Available at: https://venturebeat.com/2018/02/10/how-the-digital-divide-is-holding-the-u-s-economy-back/(Accessed January 23, 2023).

Anshari, M., Syafrudin, M., Fitriyani, N. L., and Razzaq, A. (2022). Ethical responsibility and sustainability (ERS) development in a Metaverse business model. *Sustainability* 14 (23), 15805. doi:10.3390/su142315805

Australian Law Reform Commission (ALRC) and Australian Health Ethics Committee (AHEC) (2003). *Essentially yours: the protection of human genetic information in Australia*, 280. Report No 96 (ALRC/AHEC, Sydney.

Ball, M. (2021). The Metaverse primer. Available at: https://www.matthewball.vc/the-Metaverse-primer (Accessed January 23, 2023).

Bard, A. (2020). All pyrenees. Alexander bard: and the messiah will be a machine. Available at: https://all-andorra.com/alexander-bard-and-the-messiah-will-be-a-machine/(Accessed January 23, 2023).

Bartle, R. A. (2004). *Designing virtual worlds*. Indianapolis: New Riders, 1–937.

Bartle, R. A. (2009). "From MUDs to MMORPGs: the history of virtual worlds," in *International handbook of internet research*. Editors J. Hunsinger, L. Klastrup, and M. Allen (Dordrecht: Springer), 23–39.

Bartle, R. A. (2020). CE317/CE817 lecture 1. Available at: https://www.youhaventlived.com/qblog/2021/QBlog270321A.html (Accessed January 23, 2023).

BBC News (2018). How does CCTV affect privacy in public places? Available at: https://www.bbc.com/news/technology-43702269 (Accessed January 23, 2023).

Cadieux, N., Fournier, P.-L., Cadieux, J., and Gingues, M. (2021). New techno-stressors among knowledge professionals: the contribution of artificial intelligence and websites that misinform clients. *Int. J. Electron. Commer.* 25 (2), 136–153. doi:10.1080/10864415.2021.1887695

Chouhan, C., Laperriere, C., Aljallad, Z., Kropczynski, J., Lipford, H., and Wisniewski, P. (2019). Co-designing for community oversight: helping people make privacy and security decisions together. *PACM Human-Computer Interact.* 3 (CSCW1), pp1–31. Article 146, Publication date: November. doi:10.1145/3359248

Cloudfare Inc (2022). What is the CCPA (California consumer privacy act)? Available at: https://www.cloudflare.com/learning/privacy/what-is-the-ccpa/(Accessed December 17, 2024).

De Filippi, P., and Hassan, S. (2016). Blockchain technology as a regulatory technology: from code is law to law is code. *First Monday* 21 (12). doi:10.5210/fm.v21i12.7113

Demir, H. (2021). *What is volumetric video? The future of video technologies*. New York, NY: Ant Media. Available at: https://antmedia.io/what-is-volumetric-video/(Accessed January 23, 2023).

Di Manno, J. (2021). The impact of environmental conditions on biometric authentication, Dec. 8th. Available at: https://www.fime.com/blog/blog-15/post/q-a-the-impact-of-environmental-conditions-on-biometric-authentication-344 (Accessed January 23, 2023).

Dwivedi, Y. K., Hughes, L., Wang, Y., Alalwan, A. A., Ahn, S. J., Balakrishnan, J., et al. (2023). Metaverse marketing: how the Metaverse will shape the future of consumer research and practice. *Psychol. and Mark.* 40 (4), 750–776. doi:10.1002/mar.21767

EFF, Electronic Frontier Foundation (2017). Stingrays: who's got them, who's using them, and why it matters. Available at: https://www.eff.org/deeplinks/2017/02/stingrays-whos-got-them-whos-using-them-and-why-it-matters (Accessed January 23, 2023).

Eggen, D. (2013). A guide to PRISM, the secret surveillance program under scrutiny. *Washington Post news article*. Available at: https://www.washingtonpost.com/world/national-security/a-guide-to-prism-the-secret-surveillance-program-under-scrutiny/2013/06/07/ab5adc8c-ce3f-11e2-8845-d970ccb04497_story.html (Accessed January 23, 2023).

EU (2024). "Articles of GDPR," in *2024 art. 6 lawfulness of processing*. Available at: https://gdpr-info.eu/art-6-gdpr/(Accessed December 17, 2024).

EU, European Commission (2023). Regulatory framework proposal on artificial intelligence. Available at: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai (Accessed June 09, 2023).

EU, The Aritificial Intelligence Act (2023). *Future Life Inst. (FLI)*. Available at: https://artificialintelligenceact.eu/(Accessed June 09, 2023).

Exmundo, J. (2022). *Soulbound tokens (SBTs): meet the tokens that may change your life*. NFT Now. Available at: https://nftnow.com/guides/soulbound-tokens-sbts-meet-the-tokens-that-may-change-your-life/(Accessed January 23, 2023).

Fraga, D. (2020). The manifesto of ontological design. Available at: https://medium.datadriveninvestor.com/the-manifesto-of-ontological-design-7fdb19169107 (Accessed January 23, 2023).

GDPR, European Union (2020). General data protection regulation (GDPR). Available at: https://gdpr-info.eu (Accessed January 23, 2023).

Gewirth, A. (1978). *Reason and morality*. Chicago: University of Chicago Press.

Gillespie, T. (2018). *Custodians of the internet: platforms, content moderation, and the hidden decisions that shape social media*. Yale University Press.

Goldman, B. B. (2021). The Metaverse will give designers the chance to create a better world. *Builtin Beta*. Available at: https://builtin.com/design-ux/virtual-world-design-ethics (Accessed January 23, 2023).

Grawert, J. (2015). Stingrays: the new police tool that could Be a major threat to your privacy. *Brennan Cent. Justice*. Available at: https://www.brennancenter.org/our-work/analysis-opinion/dojs-new-stingray-policy-good-start-its-got-problems (Accessed January 23, 2023).

Greenfieldboyce, N. *PRISM: what we know so far*. National Public Radio. (2013) Available at: https://www.npr.org/2013/06/07/190554149/prism-what-we-know-so-far (Accessed 23.January.2023).

Greenwald, G., and MacAskill, E. (2013). NSA Prism program taps in to user data of Apple, Google and others. *The Guardian* Available at: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data (Accessed 7 June 2013).

Hackl, C. (2020). Now is the time to talk about ethics and privacy in the Metaverse. *Forbes*. Available at: https://www.forbes.com/sites/cathyhackl/2020/08/02/now-is-the-time-to-talk-about-ethics–privacy-in-the-metaverse/ (Accessed January 23, 2023).

Hedger, J. (2019). *Kolabtree*. Available at: https://www.manufacturingtomorrow.com/article/2019/11/using-biometrics-in-industrial-control-systems/14464 (Accessed February 23, 2023).

Irwin, L. (2024). GDPR: when do you need to seek consent? *IT Gov.* 27 (June). Available at: https://www.itgovernance.eu/blog/en/gdpr-when-do-you-need-to-seek-consent (Accessed December 17, 2024).

Jurrien, I. (2021). Vivo smartphone with build-in mini drone with camera. *LetsGoDigital Rev*. Available at: https://en.letsgodigital.org/smartphones/vivo-smartphone-drone-camera/(Accessed January 23, 2023).

Kim, A., Darakjian, N., and Finley, T. (2017). Walking in fully immersive virtual environments: an evaluation of potential adverse effects in older adults and individuals with Parkinson's disease. *J. neuroengineering rehabilitation* 14 (1), 16. doi:10.1186/s12984-017-0225-2

Kleinman, Z. (2018). Cambridge Analytics: the story so far. *BBC News*. Available at: https://www.bbc.com/news/technology-43465968 (Accessed January 23, 2023).

Koops, B. J. (2014). The trouble with European data protection law. *Int. Data Priv. Law* 4 (4), 250–261. doi:10.1093/idpl/ipu023

Kozuch, K. (2022). Apple Glasses: everything we've heard so far, Tom's Guide. Available at: https://www.tomsguide.com/uk/news/apple-glasses (Accessed January 23, 2023).

Lassiter, R. (2017). *The use of CCTV in public places: balancing privacy and security*. San Francisco, CA: Electronic Frontier Foundation. Available at: https://www.eff.org/deeplinks/2017/06/use-cctv-public-places-balancing-privacy-and-security (Accessed January 23, 2023).

Le, T. (2010). *A headset that reads your brainwaves*. TED Global. Available at: https://www.ted.com/talks/tan_le_a_headset_that_reads_your_brainwaves (Accessed January 23, 2023).

Lores, E. (2021). *Achieving digital equity means tackling "tech poverty"*. Geneva Switzerland: World Economic Forum. Available at: https://www.weforum.org/agenda/2021/06/digital-equity-tackling-tech-poverty/(Accessed January 23, 2023).

Lubin, J. (2022). Blockchain comparison. Available at: https://blockchain-comparison.com/blockchain-knowledge-base/web-3/(Accessed January 23, 2023).

Madary, M., and Metzinger, T. K. (2016). Real virtuality: a code of ethical conduct. Recommendations for good scientific practice and the consumers of VR-technology. *Front. Robotics AI* 3, 3. doi:10.3389/frobt.2016.00003

Maloney, P., Freeman, G. Z., and Robb, A. (2021). Social virtual reality: ethical considerations and future directions for an emerging research space. *Conference: 2021 IEEE conference on virtual reality and 3D user interfaces abstracts and workshops (VRW)*. doi:10.1109/VRW52623.2021.00056

Molka-Danielsen, J., Rasool, J., and Smith, C.-H. (2021). *"Design and deployment considerations for ethically advanced technologies for human flourishing in the workplace" LNCS*. Springer.

Mystakidis, S. (2022). Metaverse. *Encyclopedia* 2 (1), 486–497. doi:10.3390/encyclopedia2010031

Newell, B. C. (2019). "Privacy and surveillance in the streets", In *Surveillance, Privacy and Public Space*. Editors B.C. Newell, T. Timan, and B.-J. Koops (London, New York: Routledge, Taylor & Francis Group), 1–15.

Nissenbaum, H. (2009). *Privacy in context: technology, policy, and the integrity of social life*. Stanford University Press.

Norris, P. (2001). *Digital divide: civic engagement, information poverty, and the internet worldwide*. Cambridge University Press.

Ohlhaver, P., Weyl, E., Glen, and Buterin, V. (2022). *Decentralized society: finding Web3's soul*. Available at: https://ssrn.com/abstract=4105763 (Accessed December 17, 2024).

Pearson, E. (2019). *"Why France hit Google with a whopping €50 million fine" the Local*. Available at: https://www.thelocal.fr/20190121/why-france-fined-google-50-million/(Accessed January 23, 2023).

Privacy and Human Rights Report (2017). CCTV in public spaces: balancing privacy and security. Available at: https://www.privacyinternational.org/report/cctv-public-spaces-balancing-privacy-and-security (Accessed January 23, 2023).

Privacy International (2020). The use of CCTV in public space. Available at: https://privacyinternational.org/campaigns/use-cctv-public-space (Accessed January 23, 2023).

Raine, L., and Anderson, J. (2019). *Internet of things connectivity binge: what are the implications?* Washington, DC: Pew Research Center.

REAP Technologies (2021). Machinist VR/AR training. Available at: https://www.youtube.com/watch?v=cjMqSkqvlqg (Accessed January 23, 2023).

Roettgers, J. (2021). How to build a safer, more inclusive metaverse. *Protocol, Newsletters* 19. Available at: https://web.archive.org/web/20221128012828/https://www.protocol.com/newsletters/next-up/oasis-consortium-metaverse-blomkampvolumetrics.

Silverman, D. (2015). The Stingray: a secretive and controversial surveillance tool. ProPublica. Available at: https://www.propublica.org/article/the-stingray-a-secretive-and-controversial-surveillance-tool (Accessed January 23, 2023).

Smith, C.-H. (2016). Electronic visualisation and the arts (EVA) conference, *Context engineering experience framework*. Available at: https://www.scienceopen.com/hosted-document?doi=10.14236/ewic/EVA2016.37 (Accessed 23.January.2023).

Smith, C.-H., Molka-Danielsen, J., and Rasool, J. (2020). "Transforming TELfor human flourishing: learning enhanced technology (LET)," in *IEEE TALE 2020 conference proceedings* (IEEE 2020 ISBN).

Smith, C.-H., Molka-Danielsen, J., Rasool, J., and Webb-Benjamin, J.-B. (2023). "The world as an interface: exploring the ethical challenges of the emerging Metaverse," in *The proceedings of the annual Hawaii international conference on system sciences (HICSS)*, 6045–6054. Available at: https://hdl.handle.net/10125/103367 (Accessed March 22, 2024).

Soepeno, R. (2021). "Metaverse: a potential threat to humanity and ethics," in *GCOM1304: composition I* (Sampoerna University). doi:10.13140/RG.2.2.25540.14726

Spence, E. (2008). "Meta ethics for the Metaverse: the ethics of virtual worlds, ethics of technology project," in *Research gate* (Sydney, Australia: The University of Sidney), 3–12. Available at: https://www.researchgate.net/publication/234824743 (Accessed January 23, 2023).

SSRN (2022). *Decentralised society: finding Web3's soul*. Palo Alto, CA: SSRN. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4105763 (Accessed January 23, 2023).

State of California, USA (2024). California consumer privacy act (CCPA). Available at: https://oag.ca.gov/privacy/ccpa (Accessed December 17, 2024).

Steele, C. (2019). *Google Glass, tech target*. Available at: https://www.techtarget.com/iotagenda/definition/Google-Glass (Accessed January 23, 2023).

Stephenson, N. (1992). *Snow Crash*. New York. US: Bantam books.

Takahashi, D. (2021). The ethics of the Metaverse. *Venture Beat, Jan.* 28. Available at: https://venturebeat.com/consumer/the-ethics-of-the-Metaverse-2/(Accessed January 23, 2023).

The Information Commissioner's Office (2020). CCTV in public places. Available at: https://ico.org.uk/your-data-matters/cctv-in-public-places/(Accessed December 23, 23).

Torres-Spelliscy, C. (2022). Does "we the people" include corporations? *Hum. Rights* 43 (2). Available at: https://www.americanbar.org/groups/crsj/publications/human_rights_magazine_home/we-the-people/we-the-people-corporations/(Accessed January 23, 2023).

Turkle, S. (2011). *Alone together: why we expect more from technology and less from each other*. Basic Books.

United Nations (2020). *UNICEF: a third of the world's children missed remote learning*. New York, NY: AP News. Available at: https://apnews.com/article/fd9e149fbed50d0b7d6109f22ebb161928 (Accessed January 23, 2023).

Virtual Reality Society (2022). *The ethics of virtual reality*. London, United Kingdom: Retrieved from Virtual Reality Society official website. Available at: https://www.vrs.org.uk/

VRChat Community Guidelines (2023). *Retrieved from VRChat official website*.

Wolford, B. (2022). *What are GDPR Consent requirements?* (Brussels, BE: GDPR.EU). Available at: https://gdpr.eu/gdpr-consent-requirements/(Accessed January 23, 2023).

World Economic Forum (2023). "The European Union's artificial intelligence act, explained," in *Spencer feingold*, 28. Available at: https://www.weforum.org/agenda/2023/03/the-european-union-s-ai-act-explained/(Accessed June 09, 2023).

XPRIZE, (2021). Organisation information at Available at: https://www.xprize.org/prizes/rapidreskillingandhttps://www.xprize.org/prizes/rapidreskilling/articles/the-future-of-work-pulls-closer-as-5m-xprize-rapid-reskilling-announces-semifinalist-teams (Accessed 23.January.2023).

Zama (2023). What is TFHE-rs? *Zama Bounty Program*. Available at: https://docs.zama.ai/tfhe-rs (Accessed June 12, 2023).

Zwass, V. (2010). Co-creation: toward a taxonomy and an integrated research perspective, *Int. J. Electron. Commer.* 15 (1), 11–48. doi:10.2753/JEC1086-4415150101