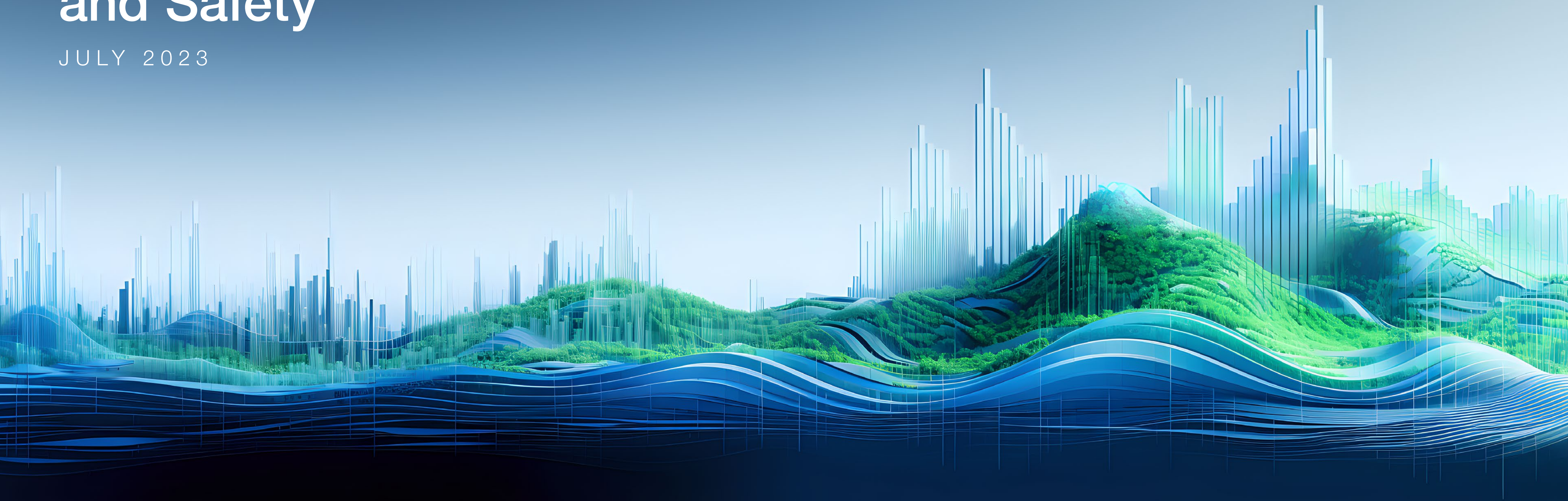


In collaboration
with Accenture



Metaverse Privacy and Safety

JULY 2023



Contents



Foreword	2
Executive summary	3
Introduction	4
Key concepts	6



1 New realities	7
2 Privacy and data processing	14
3 Engaging safely	23
4 Literacy and empowerment	41
5 Future technology considerations	44



Conclusion	47
Appendices	48
Contributors	54
Endnotes	59

This guide is interactive

Look out for this icon for pages that can be interacted with



This PDF should only be opened with Google Chrome, Microsoft Edge, or Adobe Acrobat.

Disclaimer

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

© 2023 World Economic Forum. All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, including photocopying and recording, or by any information storage and retrieval system.

Images: Getty Images, Midjourney

Foreword



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



Kathryn White
Responsible Metaverse Lead, Metaverse Continuum Business Group (MCBG), Accenture USA

The metaverse – a term used for the next iteration of the internet – continues to garner research, development, and investment interest around the world. Recent findings from Accenture indicate that the projected value of the metaverse is expected to reach \$1 trillion in the next three years, suggesting that the metaverse is already experiencing wide adoption. Furthermore, recent developments in generative AI will accelerate metaverse creation and growth, with the metaverse, in turn, providing a way for AI to reach consumers. While AI and metaverse announcements may compete for media attention, they are, in fact, partners in this digital evolution.

The need to foster international dialogue and develop directional guidance is now more relevant than ever. The previous era of technology taught us that while innovation can be a powerful force for good, it can also exacerbate existing problems and create new ones. Building upon the lessons learned from the development of the early internet, the World Economic Forum convenes thought leaders from the public and private sectors to collaboratively develop insights, strategies, and frameworks to help ensure that the metaverse contributes to economic and social progress while protecting individual rights.

This paper is a continuation of the World Economic Forum’s Defining and Building

the Metaverse Initiative. In collaboration with Accenture, past outputs from this initiative have delved into the concepts of *Interoperability in the Metaverse* and *Demystifying the Consumer Metaverse*.

We are pleased to present this second output from the governance track: Metaverse Privacy and Safety. It emphasizes key conversation areas so that the metaverse may be built with human rights, safety and privacy at its core. By presenting these insights, decision-makers are empowered to create a metaverse based on human-first principles that will positively impact individuals and society at large.

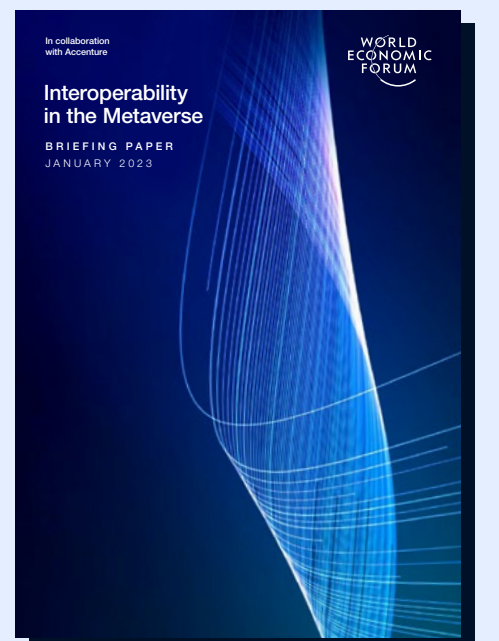
Simultaneously, the value creation track of this project has released its second output: *Social Implications of the Metaverse*. It highlights the potential consequences and new opportunities of metaverse adoption and usage on individuals. These insights should help decision-makers think about technology development from a holistic lens and incentivize outcomes for a thriving and healthy society.

Creating a metaverse that is not only economically viable, but also equitable, accessible, inclusive, and safe requires consideration of human rights, equality, and sustainability. These two publications are based on the inputs of a global, multistakeholder working group of more than

150 experts from academia, civil society, government, technology and business. The lessons from this process are informing global efforts to help realize the benefits, and mitigate the risks, of the metaverse.

Previous report:

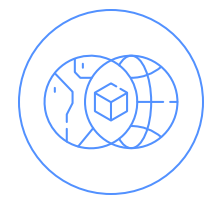
Interoperability in the Metaverse



Executive summary

The metaverse, a dynamic and interconnected digital realm, holds immense potential to reshape the way we live, work, and interact. As the convergence of augmented reality (AR), virtual reality (VR) and mixed reality (MR) blur the boundaries between physical and (semi-)virtual spaces, it becomes imperative to address privacy and safety concerns to ensure a secure and inclusive metaverse for all participants. This paper serves as a catalyst for stakeholders, promoting dialogue and action in navigating the complexities of privacy and safety in this blended world.

This paper emphasizes the importance of designing human-first experiences that prioritize the privacy and safety of all participants across the following domains:



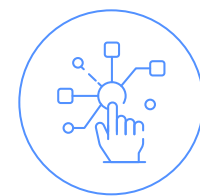
Blending worlds: Stakeholders should consider the nuances of real-world and online experiences—such as the meaning of real-world privacy vs data privacy, given the power metaverse technologies have in blending reality with digital spaces. This encompasses aspects such as rights, harms, crimes, inclusion and diversity within the metaverse environment.



Experience and environment design: Choices made today regarding platform/organizational structure, permissions levels and forum type will shape privacy practices and safety measures of participants in the metaverse.



Data processing and data privacy measures: Privacy decisions regarding the front and back end of system design play a pivotal role in cultivating trust among its users. Adequate privacy protections must be in place to ensure that individuals feel confident engaging in spatial interactions. Without robust data privacy measures, users may be reluctant to fully embrace the metaverse as a platform for social interaction, commerce and entertainment.

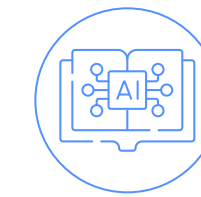


Accessing, onboarding and engaging in metaverse environments and experiences: Carefully architecting how participants access, onboard and engage is essential to delivering [privacy by design](#) (PbD) and [safety by design](#) (SbD); integral to PbD and SbD, stakeholders must consider inclusivity, accessibility and literacy design specifications.

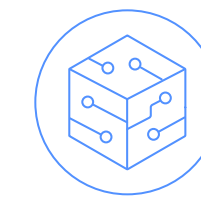


Spotlight: protecting children in the metaverse: Vulnerable groups deserve special consideration – particularly children. It is imperative to address the unique needs of children to foster a

positive and enriching metaverse experience. For example, stakeholders should consider how, when and where children's interests are supported by parental controls to promote autonomy as they grow by learning, playing and creating online.



Empowering individuals and communities with metaverse literacy: Establishing and enabling metaverse literacy is fundamental for putting human-first design principles into practice. Literacy efforts should target different education levels, be omnichannel in delivery and be customized to be persona- or demographic-specific to best empower all individuals.



Future technology considerations: While reliance on generative AI could build efficiency in populating the metaverse with infrastructure, buildings, art, personas and other objects, there is a safety risk inherent in building parts of the metaverse without responsible AI practices.

This paper highlights the importance of global cooperation and collaboration among academics, policy-makers, product design teams and regulators. It calls for a collective effort to establish metaverse literacy programmes and comprehensive frameworks that safeguard the privacy, security and rights of individuals in this dynamic digital environment.

By highlighting privacy considerations, responsible data practices and inclusive design principles, this paper aims to empower stakeholders start conversations regarding how to navigate the metaverse responsibly and ethically. Through embracing privacy-conscious practices and promoting metaverse literacy, stakeholders can unlock the full potential of the metaverse while ensuring a safe and inclusive future for all.

Introduction

The next era of the internet is on the horizon, and the “metaverse” analogy has emerged as a vision for its potential future state. Although the definition of the metaverse is continually evolving, it can be described as a collection of shared digital spaces for real-time interaction and activities – a continuum that blends digital worlds with the physical world. This paper will discuss the importance of privacy and safety considerations that can support trust and well-being in the metaverse.

The metaverse is likely to be composed of a consumer, enterprise and industrial metaverse. The early advancements towards the metaverse can be accessed through existing devices such as traditional desktops, tablets and mobile phones. In the future, however, metaverse experiences may be accessed and supported primarily by extended reality (XR) technologies – including augmented reality (AR), mixed reality (MR), virtual reality (VR) and/or other emerging technologies yet unknown.

As noted in the *State of Digital Trust* report by Information Systems Audit and Control Association (ISACA),¹ 82% of survey respondents say digital trust will be even more important in five years than it is today. For the metaverse to become a reality, all metaverse

stakeholders – including individuals and businesses – will need to address dimensions of digital trust² (see Appendix 1). Digital trust will be paramount to metaverse adoption as it is a critical building block for consumers and enterprises alike to promote a sense of safety and well-being.

The purpose of this paper is to raise awareness of privacy and safety issues within the metaverse so that [privacy by design](#) (PbD) and [safety by design](#) (SbD) approaches can be aligned with digital trust dimensions and values such as transparency, accountability, oversight, inclusive design and ethical and responsible use may be upheld. This paper seeks to educate metaverse participants, providers, creators, policy-makers and other stakeholders so that they may prioritize and mitigate potential risks. It is paramount that privacy and safety are considered for all users, both individually and holistically, and discussed with special considerations for vulnerable groups and communities, such as children. As an example, this paper includes a special spotlight on children to showcase unique conversations and risks that require special attention.





Moreover, this paper will focus on ways to design, develop and tailor “[human-first](#)” experiences in the metaverse so that all individuals can enjoy trust, safety and well-being, while navigating known digital challenges and addressing net-new metaverse challenges. While this paper focuses on surfacing safety and privacy discussion points, the scope of this paper does not cover:

- The nuanced organizational challenges of embedding trust solutions into organizations and systems
- Security and safety questions regarding metaverse identity as this will be the focus of a future report
- The need to address mental health as part of metaverse well-being; to this end, the publication [Social Implications of the Metaverse](#), published together with this paper, will help explore these topics more directly.

While the international community has recognized the importance of protecting fundamental rights³ and freedoms in the digital world, the metaverse raises new challenges requiring stakeholders to determine how the Universal Declaration of Human Rights and other foundational covenants apply. The United Nations *Guiding Principles on Business and Human Rights*⁴ and the World

Economic Forum’s *Global Principles on Digital Safety*⁵ have established the responsibility of all stakeholders in respecting and advancing human rights in digital spaces, including the right to privacy.⁶ Efforts to collectively build norms and frameworks for assessing and addressing risks related to the digital ecosystem are ongoing, and a multistakeholder approach is necessary to advance digital safety and promote human rights for all.

The early development stage of the metaverse presents a unique opportunity to prioritize privacy and safety by design, responsible innovation⁷ and human-first principles.⁸ While the metaverse is still in the early stages of development, stakeholders have a brief window of opportunity to build a digital world that embodies inclusivity, accessibility, equity, diversity and sustainability. To achieve this, stakeholders must learn from the lessons (harms, challenges and threats) of previous internet generations and go forward with purpose. A global, multistakeholder cooperative effort that reflects best values and aspirations and is built to serve the needs of all people is paramount to success.

Foundational key concepts

This paper makes frequent mentions of the metaverse, metaverse stakeholders, human-first, digital trust, well-being, privacy and safety, defined opposite.

While the concepts underlie the discussions in this paper, notions of trust, well-being, privacy and safety should be contextualized to different local regulations, cultures, customs and sensitivities.

Metaverse: The metaverse is a network of interconnected two dimensional (2D) and three dimensional (3D) physical and digital worlds and environments of (semi-)immersive nature that can be experienced with a sense of presence.

The market is still converging around on a single definition, see Appendix 2 for additional market definitions.

Metaverse stakeholders: Metaverse stakeholders: the individuals who engage with and support the metaverse.

- **Providers:** The technology, platform and service providers that build the infrastructure and devices for the metaverse.
- **Creators:** Creators make content and experiences for participants on the platforms that providers make available.
- **Participants:** Individuals who (will) participate in the experiences that creators make.
- **Civil society:** Community groups, non-governmental organizations (NGOs), labour unions, indigenous groups, charitable organizations, faith-based organizations, professional associations and foundations that have a role in public life.
- **Academia:** Communities dedicated to research, education and scholarship.
- **Government/policy-makers:** Members of government responsible for policy-making.

Human-first metaverse: A metaverse that prioritizes the human needs of the individual

and consequently integrates supportive design choices, tools and interactions to respect the persons behind the data. This transcends decisions – from architecture and security to privacy, identity and safety choices. This is an inclusive design philosophy that considers people's needs as they are, irrespective of geography, cultural identity, ability or age. It strives to be equitable and inclusive of all, not just most.

Metaverse technology:

- **Extended reality (XR):** a fusion of all the realities – including augmented reality (AR), virtual reality (VR), and mixed reality (MR) – that consists of technology-mediated experiences enabled via a wide spectrum of hardware and software, including sensory interfaces, applications and infrastructures.
- **Virtual reality (VR):** a fully immersive software-generated artificial environment. VR is a simulation of three-dimensional images, experienced by users via special electronic equipment, such as a head-mounted display (HMD).
VR can create or enhance characteristics such as presence, embodiment and agency.
- **Mixed reality (MR):** seamlessly blends the user's real-world environment with digitally created content, where both environments can coexist and interact with each other.
- **Augmented reality (AR):** overlays digitally created content on top of the user's real-world environment, viewed through a device (such as a smartphone) that incorporates real-time inputs to create an enhanced version of reality.

Metaverse environment: Also known as immersive virtual environments (IVEs),⁹ these are (semi-)immersive spaces hosted on a given platform.

Metaverse experience: The activities, engagement, transactions etc. enabled across metaverse environments.¹⁰

Privacy:¹¹ Privacy is defined as the right of an individual or entity to manage and maintain control over and confidentiality of information and data about itself, and to make choices on how that data is used and shared; the freedom from interference in one's personal affairs.

Safety:¹² Safety is the state achieved by taking actions to prevent and reduce harms. Metaverse safety includes driving responsible platform design and governance, designing tools to empower individuals to moderate their online experiences, and mitigating illegal or harmful content and conduct. It is important to acknowledge that digital safety requires a complex range of deliberations, balancing legal, policy, ethical, social and technological considerations.

Digital trust:¹³ Digital trust is an individual's expectation that digital and virtual technologies and services – and the organizations providing them – will protect all stakeholders' interests and uphold societal expectations and values. For more on digital trust, see the work by the World Economic Forum, [Earning Digital Trust](#).

Well-being:¹⁴ Well-being is a sense of health, vitality and happiness that arises from a person's thoughts, emotions and actions.

1

New realities

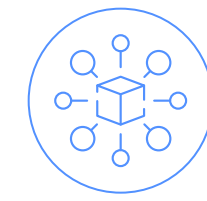


1 New realities

Privacy and safety design choices are paramount to delivering a human-first, responsible metaverse.

With new internet infrastructure, hardware devices and data types required to render AR, MR and VR experiences, stakeholders should proactively examine novel safety and privacy concepts.

These concepts are examined in the following sections of the paper. This will help identify ways to build PbD and SbD. Research by Accenture has shown that companies, researchers and governments have worked to retrofit privacy, security and other consumer protection elements into the internet – and yet they often seem to be one step behind. Therefore, it is essential to embed responsibility into the metaverse experience design.¹⁵



Decentralization¹⁶

Emerging models – from fully centralized to completely decentralized – will challenge traditional governance structures, infrastructure management and experience delivery.



Types of data

(New) types of (non-)personal, body-based¹⁷ and inferred data¹⁸ could potentially be generated, collected, processed and used, challenging privacy expectations and definitions.



(Semi-)immersive environments

Virtual and augmented worlds will enable people to inhabit spatial experiences and digital content to be overlaid on the physical world. This will help to create an enhanced sense of presence in digital spaces not previously experienced.



Interoperability¹⁹

Virtual movement across ecosystems will enable money, identities and objects to translate across metaverse environments and experiences, calling into question data management practices, jurisdictional challenges and societal norms in virtual spaces.



Blending of worlds

As physical and digital worlds increasingly blend, stakeholders need to continue considering how analogue expectations and laws of the physical world will need to translate to the digital space.

Challenging expectations from the offline world

Stakeholders should consider how analogue and digital definitions and concepts should be applied to the metaverse. For example:



Select the tabs
to discover more

Harms and crimes in the metaverse

According to INTERPOL, there is a need to define what constitutes crimes and harms in the metaverse.³⁴ Defining crime is central to creating safe spaces as law enforcement cannot police without legislation and platforms cannot actively mitigate risks without understanding the shifting types of harm.

Harms and crimes

- **Harms** are experienced wrongs but may not necessarily qualify as a crime.
- **Crimes** are actions or omissions that may be prosecuted and are punishable by law.

The World Economic Forum's work on the Global Coalition for Digital Safety,³⁵ encourages stakeholders to consider updating and harmonizing existing crime and harm taxonomies and consider the expanded scope for the metaverse. While an existing understanding of online harms and crimes includes virtual identity theft and impersonation, virtual property theft, grooming, radicalization, cyberbullying and sexual harassment, these may take an alternate form in (semi-)immersive environments, with deeper senses of presence and the use of individual and non-playable character (NPC) avatars. As such, stakeholders should consider:

- 1** How existing laws about bodily harm can be adapted to future laws for the metaverse
- 2** The conditions under which an avatar, or digital human^{36,37} can be equated with a person in the physical world may need to be developed
- 3** Whether any currently classified harms should be elevated to crimes.

This exercise of reviewing existing materials and developing a metaverse-specific harm and crime taxonomy may help stakeholders to:



Proactively identify new types of harms and crimes



Prevent, detect and respond to crimes and/or harms



Introduce policies and risk controls for privacy and safety mechanisms.

[Australia's eSafety Strategy 2022-2025](#) outlines a broad range of known and emerging harms for online safety. While not an exhaustive list, this could, for example, include protection from online harms that 1) depicts sexual exploitation or sexual abuse of children, 2) promotes, instructs or incites terrorism, violent extremism or other criminal activity, 3) encourages or promotes suicide or self-harm, 4) bullies, abuses, threatens, harasses, intimidates or humiliates another person, 5) involves non-consensual sharing of intimate images or videos, and 6) is inappropriate and potentially damaging for children to see.

Like in the physical world, harms and crimes in metaverse experiences³⁸ will be local and/or culture-specific. Moreover, unique risks may arise in different countries or regions or for different communities. The metaverse adds spatial harms – gestures, postures, digital assets and more – that will require a dedicated approach. A proactive approach to anticipate issues related to privacy and safety is essential to enable platforms and governments to safeguard users.

Blending jurisdictions

The virtual aspect of the metaverse allows people to connect in immersive spaces irrespective of where an individual resides in the physical world. This sense of digital presence begs much deeper questions around jurisdiction, such as:

- If a crime occurs in the metaverse, who has jurisdictional authority?
- What redress capability and remedies should exist, what forensic ability should be available to support it and who should be accountable for enabling the process?
- Who should be responsible for defending, protecting and hardening network infrastructure and hardware that supports metaverse experiences?

It is critical that metaverse stakeholders:

1

Consider how to address recourse and redress across jurisdictions where metaverse services are made available.

2

Establish privacy-preserving, secured communication channels to work across borders, international law enforcement and cooperation efforts safely and efficiently for intelligence collection, information sharing, mutual legal assistance and adjudication.

3

Continue to clarify what community awareness-raising and other prevention efforts, monitoring, policing, accountability, liability, enforcement and post-experience care looks like.

4

Provide enforcement and judiciary members with sufficient resources and capacity to address concerns – especially for vulnerable populations such as children.³⁹





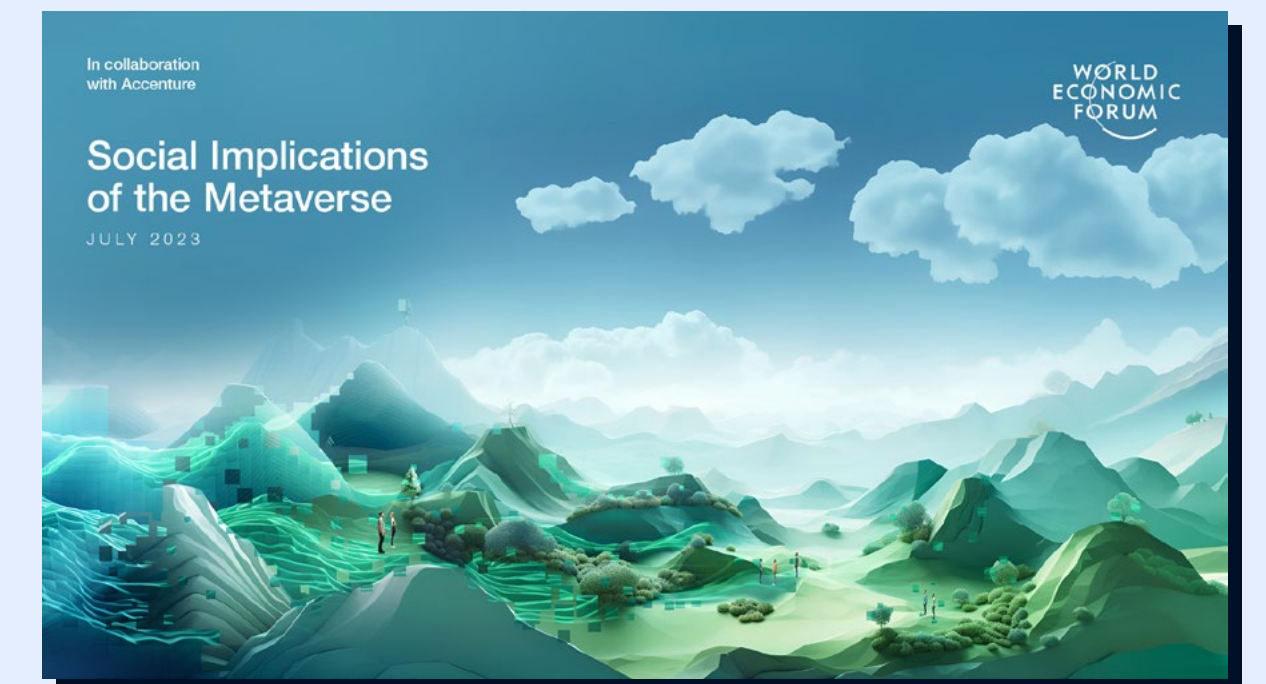
Digital accessibility and inclusion

As the world continues to blend and it becomes difficult to distinguish “online” from “offline”, it is critical to address the digital divide. Before the early 2000s, participating in social events, work and commerce meant engaging in person. Digital interaction became normalized with the rise of e-commerce. Now, as the digital world expands, it is essential to ensure that everyone has equal access to technology and digital resources. Of note, stakeholders should not forget to address vulnerable groups, economically disadvantaged persons and marginalized communities who may not be as familiar and experienced with navigating and engaging with digital worlds. These topics are addressed in *Social Implications of the Metaverse*.

Mental, psychological and emotional well-being

The impact on mental, psychological and emotional well-being must be considered. Online social communities can have a profound impact on offline social communities, both positively and negatively. Online social communities can provide a sense of belonging and support for individuals who may feel isolated or marginalized in their physical communities.⁴⁰ Conversely, online social communities can also lead to escapism and disconnection from the physical world, which can have negative impacts on mental health.⁴¹ It is essential to strike a balance between the benefits and potential risks associated with participation in online social communities. These topics are also addressed in *Social Implications of the Metaverse*.

Social Implications of the Metaverse



Experience and environment design

Choices made today regarding platform/organizational structure, permission levels and forum type will influence the privacy and safety of participants. Decisions are not binary; these environment and experience design decisions exist on a spectrum. A platform may opt to organize into a centrally managed structure with some decentralized components. This may extend to some environments and experiences being highly permissioned spaces, while some are permissionless. Moreover, a public environment may still have some private elements. To prioritize privacy and safety, stakeholders should consider the architectural advantages and disadvantages of each.

Environments and experiences may have varying degrees of centralization, permissions and management.

The list in Table 2 is non-exhaustive.



Select the tabs to discover more

TABLE 2

Basic privacy and safety considerations for metaverse environments

2

Privacy and data processing



Data processing and privacy in the metaverse

Privacy is essential for promoting trust in virtual environments and digital spaces. Without appropriate privacy protections in place, individuals may be hesitant to engage in virtual interactions, which can limit the potential of the metaverse as a platform for social interaction, commerce and entertainment.

To meet the challenges of the metaverse, stakeholders should advance data privacy⁴² by:

- Understanding the nuances of data types being processed to create and support the metaverse
- Identifying where there are existing regulatory gaps and where regulation is overlapping or contradictory to determine where metaverse-specific regulation may be needed and/or harmonized.

Processing data types

Enabling privacy is paramount in metaverse design, and stakeholders should consider how the data supply chain can and should accommodate data types being processed, as well as the interfaces collecting those data points. Some experts have suggested that metaverse and immersive technologies may generate, capture and process a greater amount of data, leading to greater risks.⁴³

Examples of novel data types that may or may not be relevant in the future metaverse are detailed opposite.

Collection and processing of these types of data can be representational of “data about me”⁴⁴ or “data about us”.⁴⁵ Some fear the ways that this type of data generated by the metaverse could be used in the future.



Select the tabs
to discover more

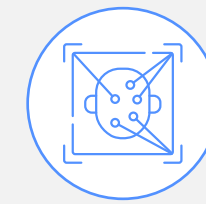


TABLE 3

Metaverse “data about me/us”

The metaverse and associated technologies may create exponential growth of “data about me/us”

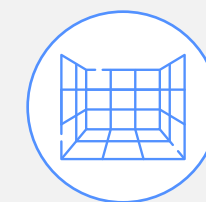
Metaverse technologies may...



Use body-based,⁵¹ biometric and other sensor data like gesturing, gait, facial expressions, eye movements, vocal inflections and vital signs in real time.



Capture and process sensitive information types⁵² and personal information (PI),⁵³ personally identifiable information (PII),⁵⁴ and personal health information (PHI).⁵⁵



Capture geospatial data for augmented and virtual reality.

...and can further...



Use neurotechnology, like neuromodulation, neuro-prostheses and brain-computer interfaces (BCIs).



Measure physiological responses⁵⁶ to create new inferred data types like psychographic data.^{57,58}

While there are meaningful reasons to collect this type of information, it may challenge privacy expectations.

TABLE 4

High-level potential advantages and risks of data collection and processing



Advantages and potential value

Personalization

Sensor data can be used to personalize AR and VR experiences to an individual's preferences, such as adjusting the content based on their emotional state or physiological responses.

Enhanced interactivity

Sensors can enable more immersive and interactive experiences, such as controlling virtual objects with hand gestures or facial expressions.

Improved safety

Sensors can enhance safety by detecting and alerting individuals to potentially harmful physiological changes, such as changes in heart rate or blood pressure.

Improved security

Sensors can be used for authentication, ensuring that only authorized individuals can access the augmented or virtual reality application.



Potential risks

Privacy concerns

The collection and use of body-based and biometric data can raise privacy concerns, particularly if the data is not securely stored or is shared without the individual's consent.

Inaccuracy

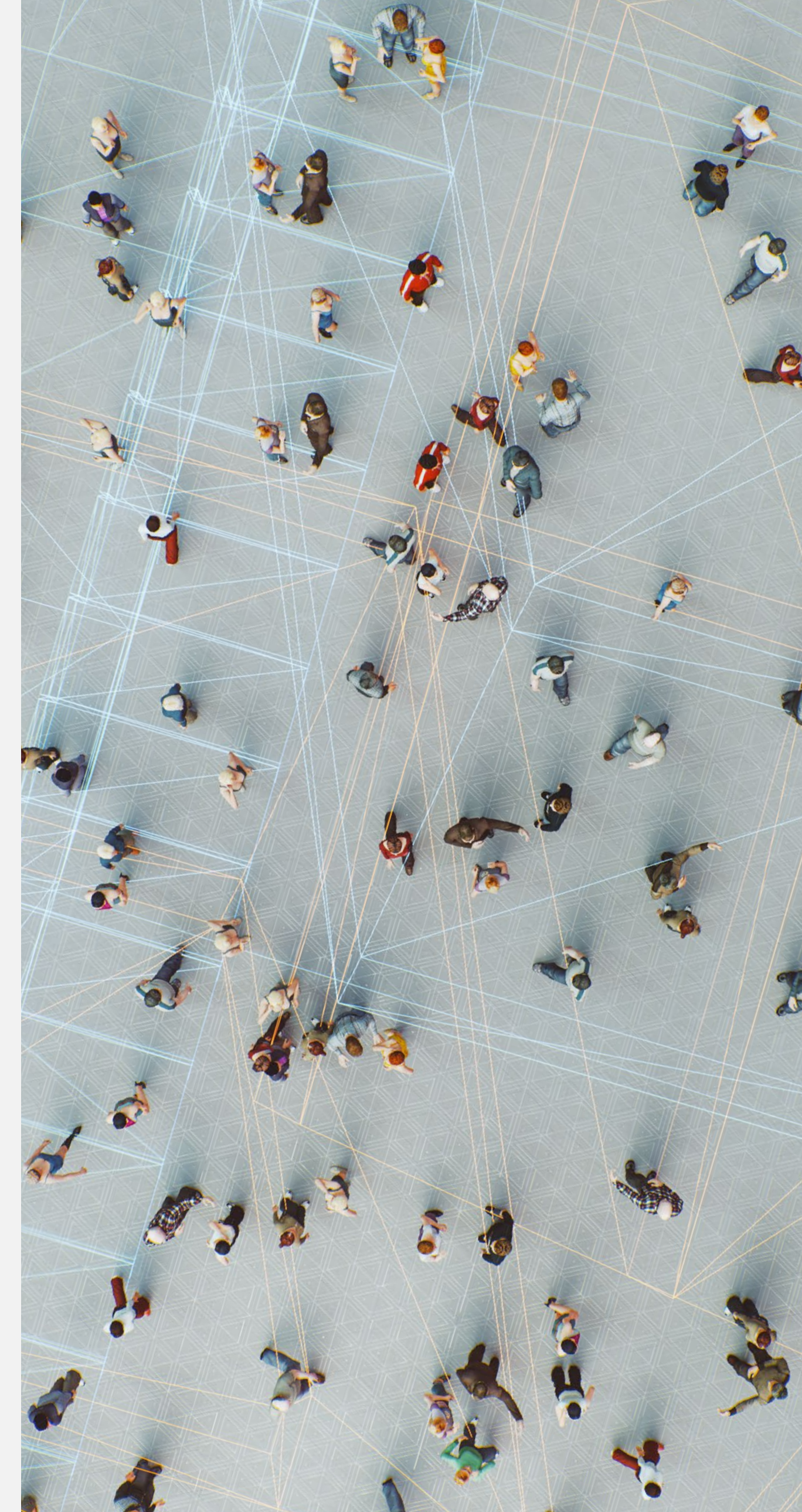
Sensors may not always accurately capture physiological data, leading to inaccurate results and potentially misleading or harmful experiences.

Ethical concerns

The use of data raises ethical concerns, particularly regarding the potential for discrimination or bias in the analysis and use of the data. Biometric data is also not replaceable in the way that a person can change a password or a lock.

Psychographics

Data can be used to track behaviour and preferences and can be correlated to other known data to create unwanted profiling, ad targeting or denial of services.



Data processing considerations

This requires that stakeholders evaluate how these data types and interfaces will interact with the data supply chain and how they will be processed. Stakeholders should review the subsequent phases.

Metaverse stakeholders should prioritize the review of data processing measures to support the safety of the individual, and work towards achieving data privacy by design (DPbD).⁵⁹ Such a review could include the actions detailed in Figure 1.

FIGURE 1

Data processing activities

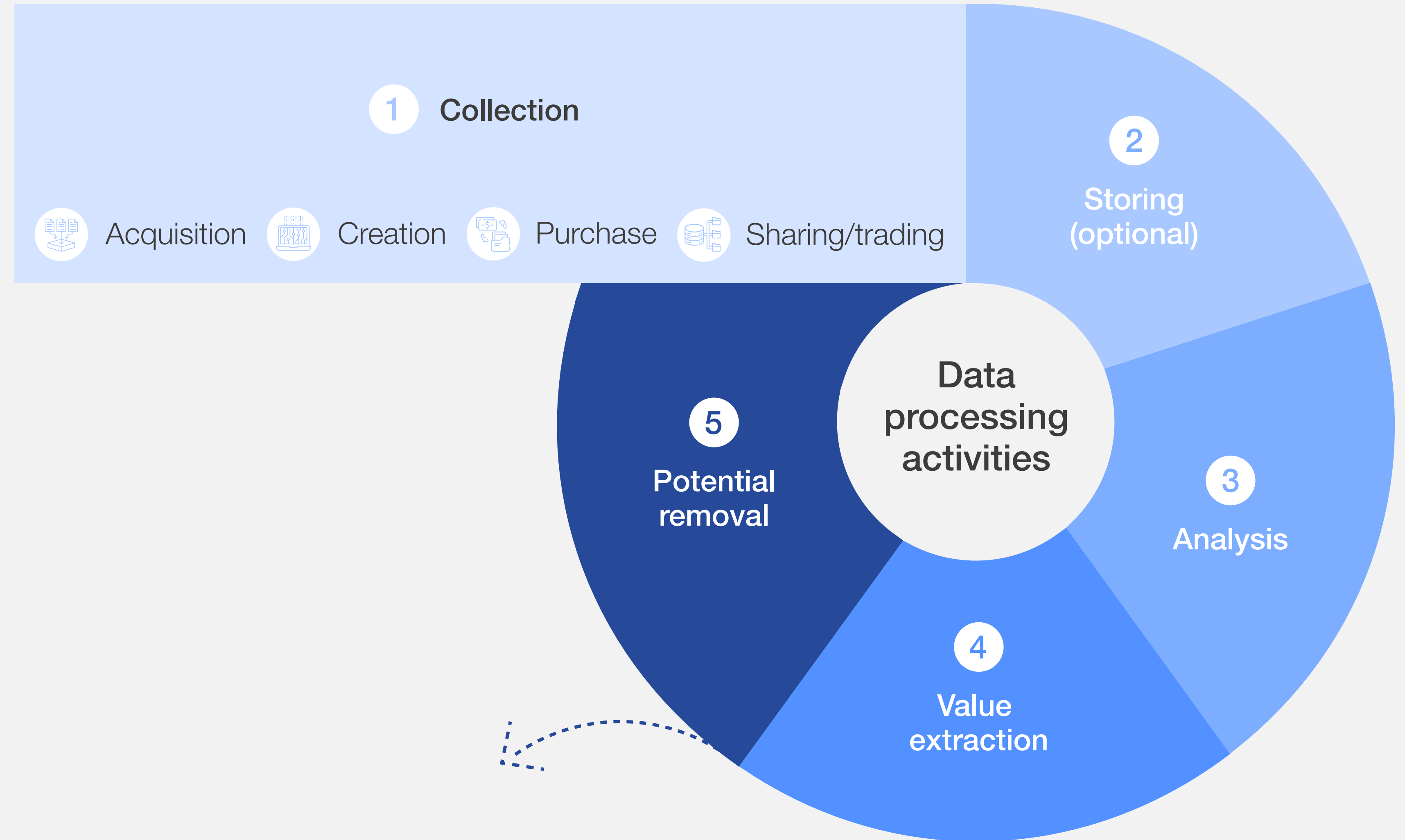


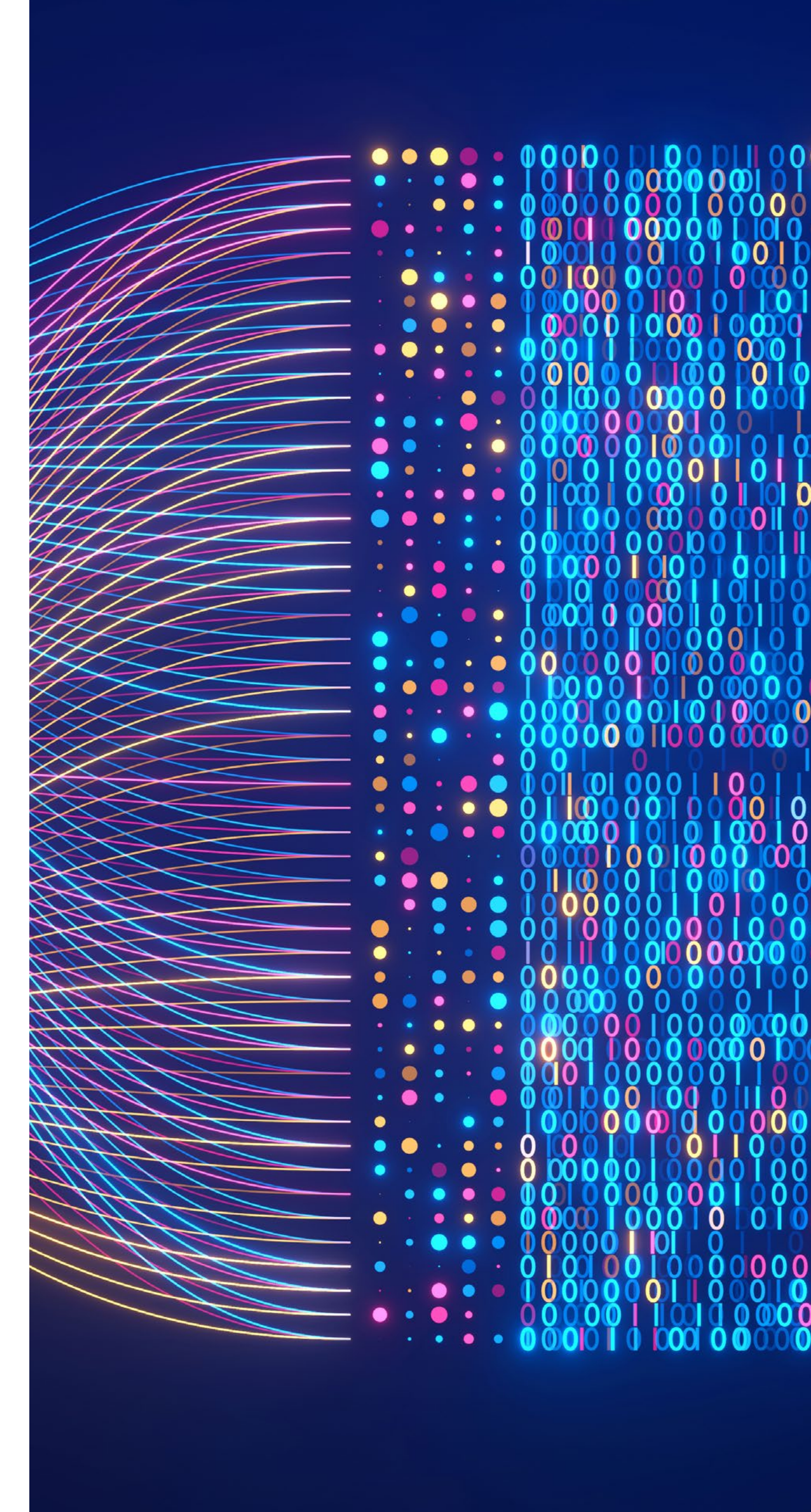
TABLE 5

Data processing considerations

Improving the data processing structure will limit the risks inherent to the collection of large volumes of data. However, data processing also requires protections around how data is regulated and used across jurisdictions.



Select the tabs
to discover more





Cross-border data flows and collaboration

A truly borderless metaverse may be dependent on interoperable components to realize economies of scale. However, a 2021 study by the Information Technology and Innovation Foundation (ITIF) found that 62 countries have bans or restrictions on cross-border data flows, and the pace of these restrictions is accelerating.⁶¹ This makes international, cross-border collaboration an imperative to streamline and protect data flows⁶² – which is a critical aspect to consider as the borderless metaverse evolves. Cross-border collaborators should continue to consider the ethical, jurisdictional and coordination implications associated with 1) novel data types and associated definitions, and 2) new types of social interactions associated with embodiment and presence.

Classification and data definitions

The diverse regional and local versions of data protection and data privacy regulations can complicate cross-border data flows, creating potential legal risks and operational difficulties for businesses. Novel data types present unique challenges and may necessitate global stakeholders to revisit data definitions to improve cross-border cooperation to fortify privacy and data protection.

Web 2.0

Personal data⁶³ is not equally defined across countries.

- The European Union’s [General Data Protection Regulation](#) (GDPR) has a **broad, horizontal** definition of personal data, encompassing any information **directly or indirectly** that may lead to a **data subject’s** identification.
- In contrast, the United States has a **sector-specific** and **state-by-state** approach to privacy laws and regulations. For example, [California Consumer Privacy Act](#) (CCPA) defines personal information in terms of data that can be **directly** linked to a **specific consumer or household**, but only covers for-profit businesses that operate in California.

Metaverse

Metaverse experiences may require the collection of data types such as (geo)spatial data to render XR experiences. It is already feasible to re-identify individuals based on this data. As a result, there may be reason to reclassify seemingly benign spatial data as personal, sensitive, PI or PII data. For example:

- A Berkeley study⁶⁴ suggests that when a VR user swings a virtual sabre at an object flying towards them, the motion data they leave behind may be more uniquely identifiable than their real-world fingerprint.
- A Cornell study⁶⁵ found that VR users can be uniquely and reliably identified across multiple sessions using just their head and hand motion relative to virtual objects.

Cross-border collaboration across the data supply chain

While existing regulations have started to address digital jurisdiction regarding concepts such as data residency, data sovereignty and data localization, the metaverse will likely require a broader privacy strategy to enable a privacy-oriented data supply chain and cross-border data flows.⁶⁶ To successfully implement a privacy-orientated data supply chain, possible solutions are detailed opposite.

Collaborative efforts across borders and industries are crucial to enabling legal conformity and are essential for paving the way for a thriving digital ecosystem that balances opportunity with responsibility.



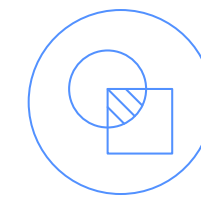
Adoption of responsible practices

Reviewing how responsible practices throughout the data supply chain can enable the safety of and protect an individual's right to privacy while permitting data flow; the Federal Privacy Council's "[Fair Information Practice Principles](#)" (FIPPs), *The OECD Guidelines*⁶⁷ and other guidance tools can be leveraged.



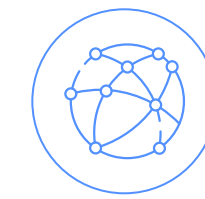
Privacy-enhancing technologies⁶⁸

Privacy-enhancing technologies (PETs), like homomorphic encryption (HE)⁶⁹ and [zero knowledge proofs](#) (ZKPs),⁷⁰ could prove to be essential tools towards increasing privacy in digital spaces if scalability challenges are addressed. However, their use alone may not fulfil human rights expectations of privacy and holistic data protection obligations.



Interoperability

Exploring the use of data intermediaries to enable broad-scale privacy and simultaneous data movement; for example, enabling auditing and assessment by independent third parties to certify data policies and practices of an organization against international standards and best practices. These certifications can then be mutually recognized internationally.



Cross-jurisdictional collaboration

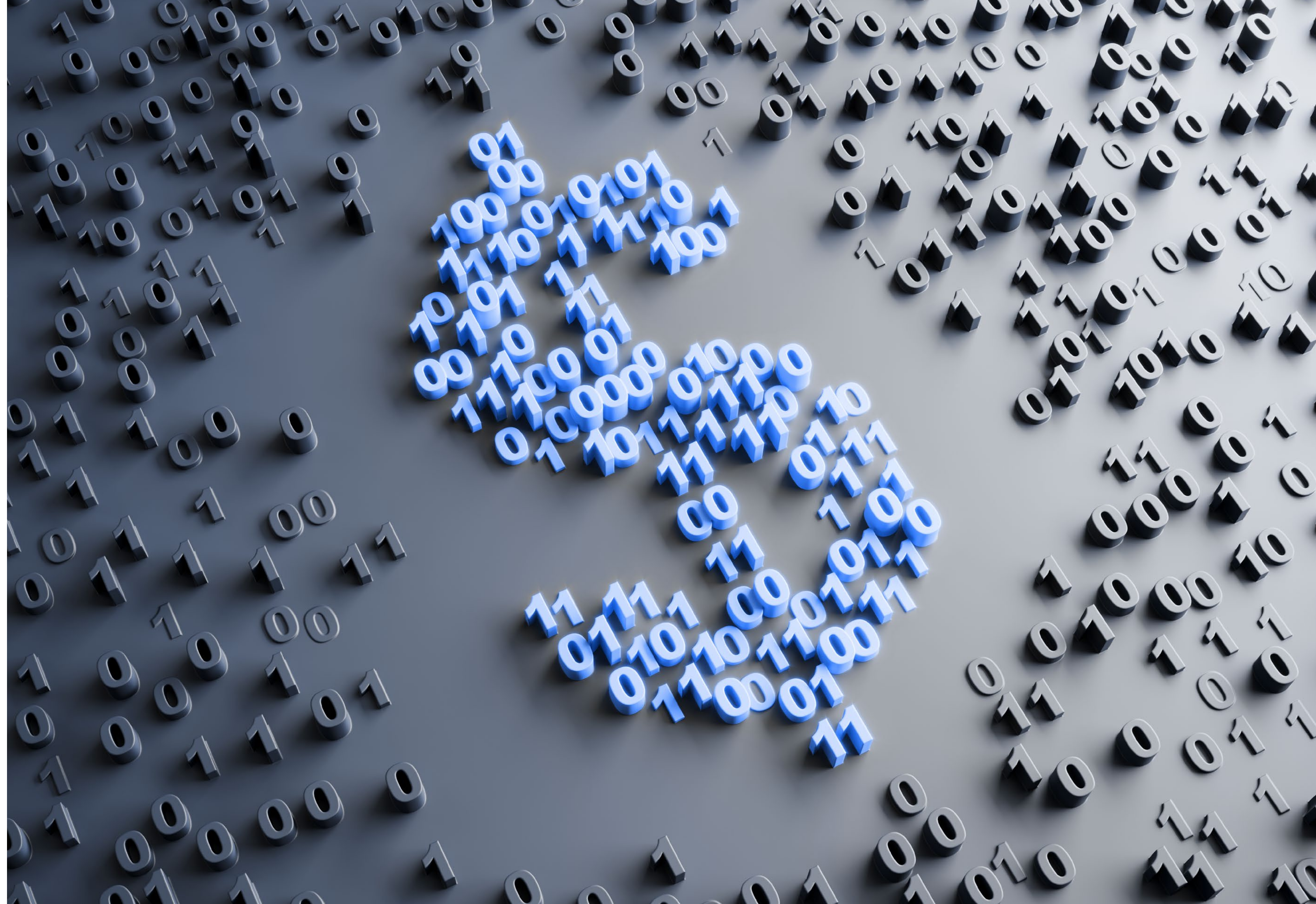
Identifying opportunities for cross-border collaboration and standardization and facilitating cross-border law enforcement access to data for recourse and redress could help harmonize approaches to developing a privacy-orientated data supply chain.



Data dependent business models

As organizations consider different business models in the metaverse, a key consideration will be how to balance the need to collect and process data to enable the functionality of the metaverse, with 1) providing optimal UX, 2) enabling responsible monetization models, and 3) addressing concerns around individual access and data privacy.⁷¹

Irrespective of what type of data may be collected, stakeholders should focus on data transparency and appropriate controls for people. Starting with data protection by design (DPbD) will enable human-first approaches to business models.



3

Engaging safely



Accessing, onboarding and engaging in environments and experiences

Privacy and safety considerations must be made at each stage of accessing, onboarding and engaging in metaverse environments and experiences. As core tenants of privacy and safety by design, those considerations must also include inclusivity, accessibility and literacy design specifications.

Moreover, carefully architecting how participants access, engage and address issues when something goes wrong is essential to protecting individual rights. Stakeholders can advance protections by considering that privacy and safety design requires an evaluation of the major safety risks associated with the specific individual journey and addressing them accordingly. This section spotlights the following non-exhaustive focus areas.

FIGURE 2
Privacy and safety



Select the icons to go to the consideration area



Physical safety of self

Whether using AR/MR in the tangible world or VR in a fully immersive world, stakeholders and participants should be aware of the safety of their physical selves.

While many AR and VR devices enable safety mechanisms like virtual boundaries, sensor warnings and safety information to combat these issues, there are additional (non-exhaustive) safety concerns that stakeholders should consider:

- Non-inclusive⁷² XR device design specifications⁷³ may cause potential injuries. Therefore, special considerations are needed for individuals with disabilities and/or motor impairments.
- Physical disorientation may cause motion sickness, falls and other accidents.
- As individuals enter a fully virtual or mixed experience, they can feel disoriented and may confuse virtual spaces and their physical surroundings, akin to dissociative disorders or derealization.⁷⁴ Similarly, AR experiences can cause inattentive blindness⁷⁵ – where individuals are hyper-focused on the AR overlay from their device

and may inadvertently cause harm to themselves or others by losing track of their physical surroundings.

- It has been proven that seeing oneself performing some action in virtual reality can change one's behaviour and memory – potentially creating false memories. It was found that children are the most susceptible to confusing memories in VR for real-world happenings.⁷⁶
- Harassment and harm of individuals wearing headsets from individuals external to an immersive experience. This may include harassment and bullying of individuals using AR in public spaces due to misunderstanding or perceived privacy infringement.
- Hacking of haptic devices causing physical sensations and feelings of invasion from a virtual harasser.

While new studies are helping redesign the technology to improve comfort and individual experiences^{77,78} balancing these accessibility concerns is critical to enabling participants to engage in safe metaverse experiences.



Back to Figure 2:
Privacy and safety

UI/UX design

Deviating from Web 2.0 interfaces, the metaverse will likely witness a greater scale and breadth of experience types requiring reimagined navigation within, between and across AR, VR and MR experiences.

When moving from place to place, individuals must have a way to make informed decisions about content and experiences. UI/UX design in the metaverse will differ from traditional gaming in the ways detailed opposite.

As a first step towards mindful design, advisory labels and clear rating systems could ways to build in warnings for individuals to promote safety.

1 Human-first design⁷⁹

In designing new interfaces and experiences, prioritizing trust, inclusion and accessibility is key to ensure that all users can fully engage with and enjoy the experiences while considering new forms of input and output, such as haptic feedback and voice recognition.

2 Well-being

With the potential for users to spend significant time in these experiences, designers should consider responsible design to prevent mindless scrolling and other harmful practices seen in traditional social media platforms.

3 Navigation

The 3D nature of the metaverse will require designers to think about spatial awareness and orientation in novel ways. Beyond the URL links of 2D webpages, interfaces and menus will need to be intuitive and easy to use in 3D spaces.

4 Customization

With greater degrees of customization and personalization, designers may need to create interfaces that can accommodate a wide range of user preferences and needs.

Notice and consent models

While there are many lawful bases for data processing,⁸⁰ the unique environments and types of data collected and processed to support immersive experiences require stakeholders to rethink how notice and consent models, or user choice frameworks, appear to participants. Stakeholders should consider developing new and innovative approaches that are better suited to the unique challenges of metaverse environments – including new interfaces, hardware and data collection points. Existing pain points of notices to address include:⁸¹ 1) text length and readability, 2) accessibility, 3) frequency and scalability, and 4) presentation and timing.

By prioritizing individual privacy and safety in consent models – and following established privacy frameworks like section 1.5 INFORM (IN) from XRSI⁸³ – stakeholders can establish a strong foundation for trust. However, consent may not always be an effective lawful basis in an interoperable metaverse environment. There are scenarios where companies collect data for legitimate interests,⁸⁴ and user consent may not be required. Legitimate interests, as explained by the European Commission, states companies sometimes need to process personal data to complete business tasks without legal obligation or contractual agreement with such persons. The use of legitimate interests still requires transparency and careful consideration of the benefits and risks of personal data use.

The goal of notice and consent should be to empower individuals to make informed decisions about the collection, use and sharing of their personal data. This can help to build trust among individuals and create more positive and engaging experiences.

Potential avenues to address pain points may include:⁸²

- 1 Evaluation of and reimagining “take-it-or-leave-it” consent to provide customized consent.
- 2 Portable, retractable consent that enables free movement across platforms/vendors and their experiences.
- 3 Use of digital agents or digital intermediaries to aid in consent processes (see the “Digital agents and digital intermediaries” section).
- 4 Visual cues and interactive elements to create more engaging and understandable notices.
- 5 Using voice and/or sound as an alternative to written notices to improve accessibility.
- 6 Leveraging the immersive and tangible nature of the metaverse to provide intuitive, on-demand data controls to users.



Back to Figure 2:
Privacy and safety



Age-based access decisions

Understanding information regarding the age of individuals accessing experiences may be integral to delivering safe and trusted environments. However, while this information can provide safer experiences to enable age-gating, cabining and more, stakeholders should consider the necessity of accessing age-related information. The implementation of age-based decision mechanisms can provide benefits and unintended consequences.

It should be noted that these safety mechanisms may not be fit for all experiences, and stakeholders should exercise judgement before implementing them. Moreover, age assurance mechanisms should be adapted to risk, reaching a balance between accuracy, ease of use (i.e. friction), privacy and security appropriate to the service.



Back to Figure 2:
Privacy and safety

TABLE 6

Overview of age-based access decisions

**Non-exhaustive*



Potential advantages

Enhances user trust in platforms

By demonstrating a commitment to user safety through age verification, platforms can build trust and loyalty among their users, leading to higher engagement and retention.

Enables age-appropriate exposure

Helps protect individuals from exposure to inappropriate content, recommendations and marketing.

Aids legal compliance

Can help digital platforms comply with legal requirements and avoid liability for facilitating underage access to prohibited content.

Promotes digital literacy and citizenship

Age-based tools can be part of a broader strategy to educate younger users about digital citizenship, encouraging responsible online behaviour from an early age.



Potential unintended consequences

Potential for age falsification or inaccuracy

Age verification measures can be inaccurate or circumvented by users who provide false information, thereby reducing the effectiveness of these systems.

Raise barriers to entry

Age verification measures can be difficult to implement, expensive and may disproportionately impact smaller businesses and start-ups.

Creates exclusion

Implementation may lead to discrimination and exclusion of individuals who are not able or willing to provide age verification information, such as those without government-issued identification.

Results in loss of privacy

Can result in a loss of privacy for individuals who are required to provide personal information to verify their age. This also increases the risk of age-based targeting.

Gating, cabining and obfuscating

Environments and experiences may benefit from the use of experience gating, cabining and obfuscating to protect participants. However, each technique carries respective advantages and risks.

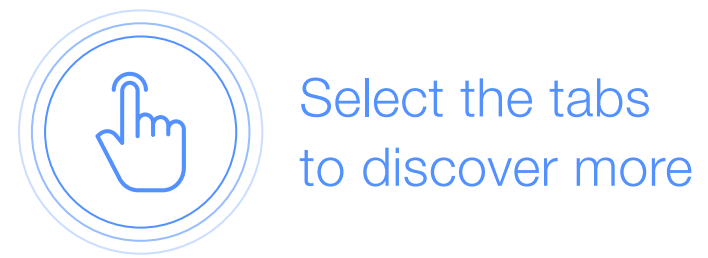


TABLE 7
Potential advantages and risks of mechanisms

Potential advantages and risks of mechanisms	

Auditing and assurance activities are necessary to verify the enforcement of these age and identity requirements.



Back to Figure 2:
Privacy and safety









Environment and experience labelling

Like video games today, environments and experiences may benefit from the use of background meta-data labels and visual cueing labels to provide contextual safety information. These can appear selectively to administrators, moderators and/or participants before and while they engage in experiences.

Some labels that stakeholders may consider are included in Table 8.

TABLE 8
Potential label types in the metaverse

Label types	Description
 Experience, content or gaming labels	Robust, age-based rating systems for various experiences that are flexible and geographically relevant based on local laws and cultural expectations.
 Location labels	Geographically accurate labels that highlight where a given individual is located.
 Identity labels	Verified ⁸⁵ and real-time authenticated labels that are tied to an individual's ID or profile, which can be used to tag adults, children and other NPCs.
 Player labels	Real-time descriptions and/or ratings that identify players based on their play style, age and/or community behaviour.
 Digital asset labels	Tags that identify objects and provide clarity on items or environmental assets being used in the space; these may be used to tag everything from fungible tokens to non-fungible tokens. Furthermore, this system may also be used to tag generated digital assets such as deepfakes.
 Advertising labels	Clear descriptions providing individuals with information on product placements, sponsorships, paid influencers and ad-related items to add authenticity and protect unwary participants.


While labelling may present an opportunity to provide information, there are potential drawbacks:

- 1 Certain label types and access to view labels may be a breach of individual privacy.

- 2 Information may not be correct, current, concise, complete or contextual – e.g. information may be out of date and/or not culturally specific.

- 3 Information may be too revelatory – e.g. an “active” status may tip people off regarding an individual’s location.

- 4 Information may not be understood if it is not immediately relevant and/or passively presented.

 **Back to Figure 2:**
Privacy and safety

Digital agents and digital intermediaries

Digital agents or data intermediaries⁸⁶ can act as trusted representatives and fiduciaries⁸⁷ for individuals, helping them to make informed decisions about the collection, use and sharing of their personal data.⁸⁸

Digital agents can be programmed to understand an individual's preferences, priorities and values and can communicate with other digital agents on the individual's behalf to negotiate data-sharing agreements. This can help to streamline the consent process and reduce the burden on individuals who may find it difficult to navigate complex and confusing consent forms. This may include the ability to adjust preferences during experiences based on content encountered and interactions made.

Data intermediaries can act as a trusted third party between individuals and data collectors, helping to facilitate transparent and fair data-sharing agreements. These intermediaries can provide individuals with clear and concise information about the data that will be collected and how it will be used and can negotiate terms with data collectors on the individual's behalf.



Back to Figure 2:
Privacy and safety



Conduct and content moderation practices

While the metaverse presents opportunities to connect in new ways with friends and peers, it also creates new avenues for malicious actors to conduct activities such as cyberbullying, grooming, harassment, social engineering, misinformation, disinformation and radicalization.

As content evolves from linear web pages and app-based experiences into (semi-)immersive avatar-led social engagements, stakeholders must proactively assess risks and create action plans for addressing how the aforementioned activities seen in today's internet might be exacerbated at scale and how they could be mitigated.

Moderating while respecting privacy

Given the discrete or impermanent nature of conduct and audio content between participants in immersive experiences, stakeholders must find privacy-preserving ways to moderate interactions while also enabling real-time enforcement of terms of service (ToS) and community guidelines. However, not all spaces or interactions require the same degrees of moderation.

Moderation is a nuanced activity that requires careful consideration and adaptation as standards, policies and regulations are formed. This is especially important and delicate with regard to balancing moderation with freedom of expression and human rights. Further research should explore how vulnerable populations – like LGBTQIA+ communities – can be supported by privacy-preserving moderation.

For example:

Private vs public moderation



Private spaces may warrant different forms of moderation. For example, should a person's speech in their virtual home be subject to the same moderation as in a metaverse environment's town square? Addressing the distinctions between public and private spaces will require refining stakeholders' understanding of content and conduct moderation and voice and expressions.

Jurisdictionally dependent moderation



Geographic regions may have different laws that will require different levels of consideration for conduct and content moderation. This may apply to the permissibility of representation, alcohol consumption, clothing choices, gestures, etc.



Back to Figure 2:
Privacy and safety



Human moderators

Moderation will likely mirror challenges faced by the gaming industry, including the challenge of resource-intensive content moderation that requires human interactions and does not scale effectively. Not only does the metaverse require sufficient human moderators to manage vast scaling environments and generated data, but it also requires ongoing consideration of the well-being of human moderators themselves.⁸⁹

Moderating for context using artificial intelligence (AI)

While AI has largely been touted as a tool to moderate the metaverse in real-time, it is essential that the use case selection and algorithm are responsible by design.⁹⁰ AI moderators must understand the context in which both conduct and content are being experienced.⁹¹

To supplement human moderators and individual reporting, metaverse stakeholders should explore how to build and implement responsible AI models that can interpret and infer patterns like humans to protect vulnerable participants from inappropriate conduct/content and improve safety. AI designers should also be conscious of issues of data bias,⁹² algorithmic discrimination⁹³ and both algorithmic explainability and transparency⁹⁴ to promote understanding of how data is processed in the algorithmic “black box”.⁹⁵

However, the call for better moderation cannot depend solely on AI implemented by platforms and third parties; moderation practices – informed by a safety-by-design approach – should empower users and assume a multistakeholder effort where everyone has access to their own moderation tools:


- All participants should be empowered with reporting mechanisms to report behaviour that breaches community standards.
- Stakeholders should consider the value of standardizing tools like muting, blocking and other safety resources.
- Organizations and human moderators should be engaged with controls and oversight at all stages of AI moderation, including recourse and redress processes and auditing processes. This will help to improve transparency.

Exiting experiences and offboarding from platforms

Exiting experiences refers to leaving a specific experience within a platform while offboarding⁹⁶ refers to completely leaving the platform and removing personal data.



Select the tabs to discover more

 **Back to Figure 2:**
Privacy and safety



Recourse and redress

The complexity of the metaverse is likely to raise the need for the development of new legal frameworks and cooperation across jurisdictions to ensure effective recourse and redress mechanisms.

For example, imagine an AR application that allows users to create and place offensive virtual graffiti on real-world buildings. This app could involve users from multiple countries, hosted on a centralized platform in one jurisdiction and using decentralized blockchain technology for content attribution and ownership. In such a scenario, questions arise regarding which jurisdiction's laws apply if the virtual graffiti infringes upon intellectual property rights or violates local regulations. If the AR application allows users to maintain anonymity, it becomes challenging to hold responsible parties accountable for their actions within the digital environment.

Mechanisms for stakeholders to consider – and jointly collaborate on – could include potential actions informed by safety by design, privacy by design and human-first principles like:



Back to Figure 2:
Privacy and safety

1. Clear, accessible, real-time reporting mechanisms for individuals to report instances of harassment, discrimination or other forms of abuse.
2. Reporting mechanisms are linked to robust investigation and enforcement procedures that can hold individuals or organizations accountable for their actions.
3. Feedback loops that inform users on the status of their reports and opportunities to appeal enforcement decisions.
4. A graduated system of sanctions and penalties for participants or organizations that violate the ethical guidelines and regulations, which are set out clearly for users in ToS and community guidelines.
5. A neutral and independent body to oversee the enforcement of ethical guidelines and regulations.
6. Support to individuals who experience harm through access to third-party support services and in-app/platform links to additional information.
7. A culture of accountability and responsibility among users of the metaverse, emphasizing the importance of respecting the rights and dignity of others and of reporting any harmful behaviour.

Respecting metaverse participants by enabling recourse and redress is essential to creating a human-first metaverse



Toxic behaviour in competitive activities is not a new development... with technological advances in online multiplayer games and video gaming's increased prevalence worldwide, a growing percentage of the population is becoming unwittingly exposed to a slew of abusive acts that are only becoming more visible.⁹⁸



While game publishers, console makers, online voice-chat applications and even the FBI are aware of these issues and working to confront them, complications stemming from modern technology and gaming practices, freedom of speech concerns and a lack of chargeable offences on the legal side make toxic elements a challenge to extinguish.⁹⁹

Spotlight: Protecting Children

To create inclusive, accessible, diverse and equitable spaces, many vulnerable groups deserve special consideration – these can include the elderly, minorities, LGBTQIA+ people, disabled persons and/or individuals with other recognized accessibility conditions, etc. As dialogue evolves on how to best consider each population in the metaverse, it is paramount to understand that vulnerable groups are distinct: the unique needs of an elderly minority person with a health condition will not be the same as those of a child who identifies as LGBTQIA+.

This spotlight highlights high-level, special considerations for children. Considerations for other vulnerable groups of people are discussed in the *Social Implications of the Metaverse* report.

Defined by the Office of the High Commissioner of Human Rights Convention on the Law of the Child as those below the age of 18,^{100,101} children are still developing, and have a right to special protection from harm. This creates an imperative for stakeholders to safeguard their foray into the metaverse to mitigate the long-term consequences of an ill-designed metaverse built without their regard.

A joint project by UNICEF and the LEGO Group, [Responsible Innovation in Technology for Children](#), is demonstrating the role that positive digital experiences can play in enhancing growth and development in children. It is increasingly clear that the best digital worlds are those that not only mitigate harm but also empower children, nurture creativity, build competence, promote diversity and inclusion, develop emotional regulation, encourage social connection, and help them self-actualize.

As a first step, organizations should evaluate their data ethics practices, governance processes, guiding principles and SbD practices to guide exploration on how children are empowered or disenfranchised.

As these issues are considered, it is important to remember:

- Solutions require multistakeholder engagement. For example, the LEGO Group has a responsible child engagement team that considers risks to children and interfaces with product teams to ensure they are considered in design choices. SbD requires a multidisciplinary approach where technical, policy, legal and marketing staff or community members can appreciate and address ethical issues together.
- Present-day challenges regarding children’s privacy, safety, trust and well-

being are being responded to via policy frameworks that can be applied to Web 3.0 and the metaverse to a degree. These frameworks will need to be updated and implemented properly, and new frameworks may be needed.

The LEGO Group, in partnership with Epic Games, developed three principles for building safe play opportunities for children:¹⁰²

-  Protect children’s right to play by making safety and well-being a priority.
-  Safeguard children’s privacy by putting their best interests first.
-  Empower children and adults with tools that give them control over their digital experience.



Considering child-specific XR device design choices

There are physical risks when using XR hardware. For children, this is magnified. Device manufacturing and software design should consider the choices opposite.



A child-friendly UI experience that includes ensuring notifications and controls are understood and navigable by children of different ages.



Increased safety protocols for children's potential lack of coordination and spatial awareness.¹⁰³ These measures may include magnified alarms for the crossing of a given boundary or stricter protocols in the setting up of a given boundary.



Specific devices designed for children,¹⁰⁴ including devices designed for the physical characteristics of a child's head and eyes.



Research into the impacts that participating in (semi-) immersive experiences may have on children's development and the use of that information to inform policy.





Enabling child consent and parental controls

Under GDPR Article 8, individuals who hold parental responsibilities can provide consent for children under 16; however, Member States can lower that age to as low as 13.¹⁰⁵ A child's ability to meaningfully consent should be considered at every stage of the metaverse experience. While parental controls can provide a base level of control in an environment where children cannot protect themselves, stakeholders should consider how, when and where children's interests are supported by such parental controls.

Considerations for parental controls include:

- Engagement, education and guidance of parents to deliver child-positive digital experiences.
- Application of digital AI guardians who can act as a proxy for decision-making based on specified requirements to reduce the burden on parents.
- Required parental supervision and guidance during the child's onboarding process, such as adult participation in the setup and associated consent process.

- Enabling optional (age-appropriate) parental supervision via secondary screens, devices or privacy settings.
- Safeguards around financial transactions and a limitation on spending by children
- Amount, quality and context of notifications sent to parents to avoid inundation.
- “Best Interest of the Child Framework”¹⁰⁶ encompasses respect for teens' evolving expectations of privacy and mechanisms to promote their autonomy as they grow by learning, playing and creating online.

While having parental guidance and controls may be necessary, it is imperative that these controls are respectful of children's rights and are age appropriate.¹⁰⁷ Where applicable, parental controls must not serve to restrict children's right to participation. For example, while a guardian may wish to prohibit a 2-year-old from entering the metaverse and should be empowered to protect their custody, it may be ill-advised for a parent to have total control over a 17-year-olds' metaverse experience. For this reason, parental supervision mechanisms must be implemented with consideration of context and a baseline understanding of what experiences children have a right to participate in.

Creating child-safe environments

Stakeholders need to consider the right of children to participate and associate online. Age gating should not create unnecessary barriers to expressing this right, as children’s well-being can be enhanced via positive digital play.

Stakeholders must design spaces-for-all where children are likely to enter with safe design that is inclusive of their participation, which could be done by:

- Making environments fit for purpose and designed with children in mind, for child-specific spaces, stakeholders should consider what options would be available to protect them
- The use of device settings that auto-opt an individual in for a “safety bubble”
- Certification of experiences by a third party to ensure that experience ratings and labels are accurate to ensure that platforms do not use adult-only content ratings to absolve them of their requirement to protect children in experiences.

As harm may occur to children in experiences, reporting mechanisms must be child-friendly and accessible for younger audiences. This can be improved by:

- Creating recourse and redress processes that are graduated, easy to understand and intuitive
- Providing parent(s) or guardian(s) with a notification when such a process begins and including them in the process moving forward.

Environments designed for children should consider the well-being and development of a child. Aside from mitigating risks, responsible design requires an assessment of the overall best interests of the child at every stage, and stakeholders should make this a priority.



Child-specific privacy considerations

Data privacy for children is nuanced, and considerations should be adjusted as a child develops.¹⁰⁸ Balancing privacy and online safety needs is a necessity. It is possible to monitor and maintain more control over online experiences at the cost of a child's privacy.¹⁰⁹ Solutions that reach the right mix between these competing policy objectives are to be preferred.

Data processing and data privacy mechanisms can be improved for children via:

- Enabling parents, (digital) guardians¹¹⁰ and/or caretakers to provide informed consent for children where appropriate based on age
- Establishing child assent models¹¹¹ so they can participate in consent structures while enabling parents the final decision
- Using data minimization, differential privacy and other privacy enhancing technologies (PETs) to prevent unnecessary data processing.

Children's data requires special consideration in the metaverse



Data, if used responsibly, can solve social problems and challenges while offering tremendous potential for innovation ... Children, however, are more vulnerable than adults and are less able to understand the long-term implications of consenting to their data collection.

Pedro Hartung, [The children's rights-by-design standard for data use by tech companies](#), UNICEF, 2020.



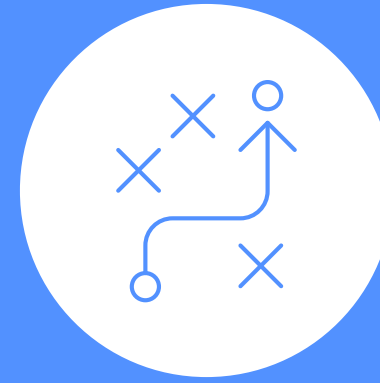
Child-specific metaverse literacy considerations

While metaverse literacy is a key component of metaverse trust and well-being for all stakeholders, children must receive education on the metaverse. The following insights are specific to metaverse literacy and awareness for children entering the metaverse. These are adapted for the metaverse based on UNICEF’s “Digital literacy for children – 10 things to know”.¹¹² Metaverse literacy goes beyond technical know-how. It refers to the skills and attitudes that empower children in an ever-increasing digital world.

Child-specific metaverse literacy should consider how best to embed literacy into experiences; additionally, stakeholders should consider providing incentivized education structures so that children and parents are motivated to learn and upskill.



Child safety programmes would benefit from greater coordination; knowledge across programmes is not systematically generated or shared.



Implementing digital literacy is not easy; key barriers include a lack of teacher, training and instructor capacity, lack of ICT infrastructure, low connectivity, and a lack of understanding from decision-makers.



Extending digital literacy will require policy development support, metaverse-specific literacy framework development, curriculum guidelines and practical considerations like teachers, technology resources and support from metaverse stakeholders.



Some existing digital literacy frameworks or tools may suit child-focused learning well – including the DigComp Framework,¹¹³ [“Get Digital: Safety in the Metaverse”](#) and [“Digital Kids Asia-Pacific Framework”](#).



Digital literacy programmes should be context-driven. Metaverse literacy will not be one-size-fits-all and should be developed and implemented within the context of the community of children participating in metaverse experiences.



Global action for protecting children in the metaverse

The following is a non-exhaustive list of regulations, standards, guidance, frameworks and best practices that are applicable to children.

4

Literacy and empowerment



Empowering individuals and communities with metaverse literacy

Promulgating metaverse literacy is essential to keeping metaverse stakeholders safe. As with digital literacy,¹²¹ staying safe and secure in metaverse experiences is a continuous effort that is multi-faceted, ever-evolving and relies on the inclusion of all stakeholder groups. Metaverse literacy must be available for all, be demographic-specific, include foundational training and enable participants to make their own informed decisions thereafter.

To enable this vision for metaverse literacy, stakeholders should make learning and development a central part of a long-term planning strategy.¹²² Critically, this strategy should target different education levels, be omnichannel in delivery and be customized to best empower all individuals – from digital natives and non-natives to children and established professionals.

Moreover, metaverse literacy should enable specific upskilling to allow key stakeholders **to embed responsible design** across development and experience delivery, regulation, standards, guidance, and best practice setting, and interventions.

Since the metaverse is blurring the line between the physical and virtual world, law enforcement and information-sharing bodies should be included in metaverse literacy campaigns to understand how to best protect rights established in the physical world in digital spaces.¹²³ In addition to participating in ongoing discussions, metaverse stakeholders should actively work with institutions to facilitate safety across the physical and digital world.





General participant education

Metaverse literacy...

Developer and experience delivery education

Stakeholders should define developer guardrails that prioritize human-first safety, which can be:

- Set via standards established through engagement across sectors – including lawmakers, standards bodies, academia and business – to share information so that safety measures can be established with meaningful understanding.
- Delivered through guidebooks and other tools – to educate metaverse providers, creators, and others in privacy-by-design and safety-by-design principles, immersive design principles,¹²⁹ accessible design¹³⁰ and creating inclusive experiences.¹³¹

This will enable developers to create welcoming cultures and responsible content.

Moreover, given the emphasis on the metaverse as an immersive learning tool, metaverse literacy should cover how to design learning environments.¹³²

5

Future technology considerations



Safety in metaverse marketplaces

As the metaverse rapidly evolves, stakeholders must address the complex challenges regarding IP, ownership, portability and safety of digital assets in a borderless digital realm. The absence of a cohesive international agreement on digital asset ownership leaves participants vulnerable to loss of data, money and objects¹³³ and highlights the need for global collaboration to establish the necessary policy and infrastructure to enable secure digital commerce.

A comprehensive understanding of IP, digital ownership and portability, alongside the development of a robust legal framework, could promote economic safety and innovation within the metaverse,¹³⁴ enabling the seamless transfer of digital assets and ensuring that the rights of all market participants are protected. Limited trade agreements on digital ownership could hinder metaverse adoption. Therefore, global collaboration is necessary to establish infrastructure, payment rails and other ways of operating for borderless commerce.

IP and ownership rights

IP protection and ownership rights are paramount in maintaining marketplace integrity, and ongoing legal precedents continue to shape the landscape for individual and brand safety. To ensure marketplace integrity and participant safety, IP protection must be prioritized. Stakeholders must explore emerging technologies for monitoring, reporting and enforcing IP while respecting privacy. Significant questions about provenance, individual-generated content, appropriation and portability of IP still need to be answered. For example, in Nike vs StockX,¹³⁵ Nike stated that “StockX’s use of Nike’s marks is, upon information and belief, intentionally deceiving consumers into believing that Nike sponsors or approves of the Vault NFTs”. In Hermès International vs Mason Rothschild,¹³⁶ Hermès claimed that Mason Rothschild’s unauthorized MetaBirkins NFTs infringe Hermes’ trademarks in the word “Birkin” and in the design and iconography of the handbag. The jury returned its verdict on 8 February 2023, in favour of Hermès. These cases highlight the need for consumer protection, brand safety and a robust legal framework to navigate the complexities of digital asset ownership.

Portability

Addressing asset ownership, protection, and portability is crucial for stakeholders. By creating a framework for transferring digital assets across various metaverse experiences, market participants can better understand the safety and privacy of their ownership. Considering scenarios such as transferring purchased assets between platforms or paying royalties to original creators when reselling digital assets, highlights the importance of examining the relationship between digital ownership and portability for ensuring economic safety.

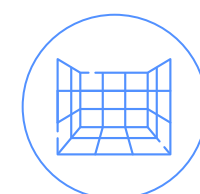


Generative AI

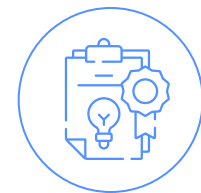
According to the International Telecommunications Union (ITU), AI may be the most crucial piece of the metaverse “puzzle” because of its potential to enable the metaverse to scale.¹³⁷

Generative artificial intelligence¹³⁸ is a new type of artificial intelligence technology that learns from past data and can generate new content in the form of text, images, videos, audio, 3D models and even computer code.¹³⁹ There will be many intersections between the metaverse and generative AI in the future,¹⁴⁰ some that cannot be predicted at this early stage.

Future technology considerations for metaverse safety include:

 If metaverse environments in the future are built by generative AI tools,¹⁴¹ there must be mechanisms in place to ensure that those environments are being auto-populated with privacy safety as core tenets. As with any automated process, it is critical to be intentional. This requires stakeholders to review focus areas across generative AI problem/use-case

design, model build, model use and post-deployment activities – namely emergent behaviours,¹⁴² hallucinations,¹⁴³ model toxicity,¹⁴⁴ regarding harmful and/or biased outputs, data poisoning,¹⁴⁵ as well as liability and compliance questions.¹⁴⁶

 There is already uncertainty about the ownership of AI-generated works, and the legal system is being asked to clarify the bounds of what is a “derivative work” under intellectual property laws.¹⁴⁷ For content created in the metaverse using generative AI, intellectual property considerations may need to be a core tenet.

While reliance on generative AI could build efficiency in populating the metaverse with infrastructure, buildings, art, personas and objects, there is a safety risk inherent to building parts of the metaverse “automatically”.¹⁴⁸ Careful consideration of ethics, liability, accountability and responsibility are needed before electing to use generative AI to build another emerging landscape. In response to needs like this, the World Economic Forum’s AI Governance Alliance is a multistakeholder initiative championing responsible global design and release of transparent and inclusive AI systems.

Experts have proposed the following early safety considerations for a metaverse underpinned by generative AI:



Continue to practise responsible AI¹⁴⁹ across dimensions such as soundness, fairness, transparency, accountability, robustness, sustainability and data ethics. These will continue to enable stakeholders to manage governance, training and risk controls for generative and predictive AI in the metaverse.¹⁵⁰



Use a tagging system for both content and individuals in virtual spaces to enable transparency and provenance to better distinguish: 1) which avatars represent people and which are NPCs, and 2) what content was produced by a physical person vs a generative AI model.



Digital literacy efforts to educate participants on the common misconceptions of factual accuracy, impartial reasoning, novelty and perceived emotional intelligence that generative AI models may demonstrate.

Conclusion

Given the opportunities for stakeholders to champion a human-first metaverse, the World Economic Forum is collaborating across business, government, academia and civil society to identify key themes for privacy and safety.

Trust and well-being, which includes components of privacy and safety, should be informed by a human rights lens. A human-first metaverse includes considerations of the International Bill of Human Rights, including the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the International Covenant on Economic, Social and Cultural Rights, as well as the World Economic Forum's *Global Principles on Digital Safety*, among other human rights frameworks.

Considerations for privacy and safety in the metaverse include the following:

- **Privacy and safety in the metaverse will transcend the physical and digital worlds.** Trust and well-being in the digital and physical worlds will continue to merge. Stakeholders should consider how standards, policies, regulations and guidance each work across the physical and digital worlds to improve people's trust and well-being both inside and outside of the metaverse.

- **Data processing in the metaverse presents an opportunity to continue to provide greater protection over individual data.**

The amount of data collected will be immense, raising potential new risks but also providing an opportunity for individuals to have greater control over data sharing and processing.

- **Safety and privacy must be protected via “by-design” processes during metaverse onboarding, within experiences and beyond.**

This is inclusive of understanding fully and accepting a platform's terms of service, acknowledging community guidelines, and setting expectations for moderation in each experience. Stakeholders should consider how to address individuals' safety and privacy expectations at every stage, as well as what role technology may play in moderation.

- **At each stage of design, the specific cases of children and other vulnerable users must be considered.**

Metaverse stakeholders should build holistic experiences that prioritize the safety and privacy of children and their overall well-being. This means building metaverse experiences where children's developmental needs and their right to play are considered at critical design stages and, where needed, balanced with the risk of harm.

- **Digital and metaverse literacy is imperative for overall trust and well-being.** Metaverse stakeholders that lack critical information cannot set reasonable expectations, respond to issues that arise or understand their rights before, within and after a metaverse experience. Stakeholders should invest in metaverse literacy as a critical component of promoting metaverse hygiene, trust and well-being.

- **It is essential to apply responsible AI practices to generative AI,** especially when being used to for power and populate metaverse experiences and environments.

Businesses, governments, academia and civil society should proactively collaborate to build and support appropriate standards and policies that support metaverse safety and privacy and take a human-first approach enmeshed in human rights considerations while furthering needed innovation in this burgeoning field. Ultimately a successful metaverse will be one that promotes trust, well-being, privacy and safety.



Appendices

A1: Digital trust framework



Source: World Economic Forum, *Earning Digital Trust: Decision-Making for Trustworthy Technologies*, 2022, https://www3.weforum.org/docs/WEF_Earning_Digital_Trust_2022.pdf.

A2: Market metaverse definitions

Entity	Metaverse definition
Accenture	Represents a continuum of digitally enhanced worlds, realities and business models. It is a dynamic environment that uses spatial computing platforms, generative AI, Web3 and blockchain technologies to enable augmentation of the real world.
European Parliament	An immersive and constant virtual 3D world where people interact by means of an avatar to carry out a wide range of activities.
Matthew Ball	A massively scaled and interoperable network of real-time rendered 3D virtual worlds and environments, which can be experienced synchronously and persistently by an effectively unlimited number of users with an individual sense of presence, and with continuity of data, such as identity, history, entitlements, objects, communications and payments.
Meriam-Webster Dictionary	A persistent virtual environment that allows access to and interoperability of multiple individual virtual realities.
Meta	The next evolution in social connection and the successor to the mobile internet.
Responsible Metaverse Alliance	A persistent and immersive, simulated or virtual world that is experienced in the first person by large groups of simultaneous users who share a strong sense of mutual presence.
Wikipedia	A hypothetical iteration of the internet as a single, universal and immersive virtual world that is facilitated by the use of virtual reality (VR) and augmented reality (AR) headsets. In colloquial usage, a “metaverse” is a network of 3D virtual worlds focused on social and economic connection.
XR Safety Intelligence	A network of interconnected virtual worlds with the following key characteristics: presence, persistence, immersion and interoperability.

A3: Human rights in the metaverse

Respecting human rights in the metaverse is critical to establishing metaverse privacy and safety.

As the digital world begins to mirror the physical world, it is necessary to extend expectations of human rights

Universal Declaration of Human Rights Article	How it applies to privacy and safety in the metaverse
Article 3: Everyone has the right to life, liberty and security of person.	Security of personhood should be defined and applied for virtual spaces.
Article 5: No one shall be subjected to torture or to cruel, inhumane or degrading treatment.	Metaverse safety measures should be geared toward protecting people from inhumane and degrading treatment.
Article 8: Everyone has the right to an effective remedy by the competent national tribunals.	Should terms of service for privacy and safety be violated, upholding this human right requires recourse and redress by either the metaverse operator and/or national governing bodies.
Article 12: No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks.	Individuals have a right to experience privacy in metaverse spaces – this equates to having digital ethics, data ethics and AI ethics applied across the data supply chain so that individuals can provide knowledgeable consent, can control access to “data about me”, have a right to be forgotten and can be free from unwanted surveillance.
Article 13: Everyone has the right to freedom of movement.	People should be able to move freely through the metaverse.
Article 17: Everyone has the right to own property alone as well as in association with others. No one shall be arbitrarily deprived of his property.	People should have security of ownership of their digital assets.
Article 19: Everyone has the right to freedom of opinion and expression.	People should be able to freely express their opinions.
Article 20: Everyone has the right to freedom of peaceful assembly and association.	People should be able to gather peacefully and associate peacefully with groups of their choosing.
Article 26: Everyone has the right to education.	People should have access to education and access to education about the metaverse.
Article 27: Everyone has the right freely to participate in the cultural life of the community.	People should feel safe to express their culture alongside their chosen community.

A4: Privacy-enhancing technologies

Privacy-enhancing technologies (PETs) are multifarious, and exactly how they could be used for metaverse applications will vary significantly by use case. They may hold potential for helping to build privacy-protective experiences in the metaverse. A non-exhaustive list of PETs is detailed opposite.

1. **PETs should be used in conjunction with data minimization** strategies.
2. Many PET use cases involve personal data; **even when PET techniques are deployed, its essential to assess how to meet all data protection obligations.**
3. The **deployment of PETs should consider the nature, scope, context and purpose** of the data processing.
4. Anonymization and PETs are separate but related concepts. Not all PETs result in effective anonymization.

Privacy enhancing technologies (PETs):

Are technologies that assist in mitigating data privacy risks; they are closely linked to the concept of “Data Protection By Design” (ICO). They are multi-purpose: 1) they can reinforce data governance choices, 2) serve as tools for data collaboration, and 3) enable greater accountability through audit. (Royal Society)

Category	PET tool	Description
Reduces identifiability of individuals	Differential privacy	Randomizes, or applies “noise” to, a person’s associated data to mitigate re-identification of an individual
	Synthetic data generation (SDG)	Uses existing knowledge to create completely fabricated “new” data
Shield and hide data	Homomorphic encryption (HE)	Allows computation to be preformed on encrypted data without revealing plain text
	Identity-based encryption (IBE)	Enables message encryption from a sender to a receiver without the use of traditional public key infrastructure (PK) by instead relying on private key generation (PKG)
	Zero-knowledge proofs	Allows statements of truth to be verified without exposing information
Split datasets or control access	Trusted execution environments	Enables secure access to cryptographic keys and sensitive data in plain text, without compromising data confidentiality – also known as a secure enclave
	Secure multi-party computation (SMPC)	Carries out distributed computing prioritizing correctness and minimally viable learning of inputs and outputs to secure the computation process
	Private information retrieval (PIR)	A multi-party computation (MPC) protocol allowing users to query a database while hiding the identity of the data retrieved
	Private-set intersections (PSIs)	SMPC cryptographic technique that allows comparison of encrypted information across parties to derive information from an intersection point
	Federated learning	Empowers individual endpoints to participate in machine learning model training while keeping the training data on device and sending only summary data to a centralized data store

A5: Privacy and safety frameworks

A comprehensive framework to safeguard humans and societies in the metaverse will enable well-being and trust. One such framework is the [XRSI Privacy and Safety Framework](#).



Select the buttons
to discover more

Source: “The XRSI Privacy and Safety Framework 2”, *XRSI*, n.d., <https://xrsi.org/definition/the-xrsi-privacy-framework>.

Contributors

World Economic Forum

Minos Bantourakis

Head, Media, Entertainment and Sport Industry

Daniel Dobrygowski

Head, Governance and Trust

Cathy Li

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

Aiden Slavin

Lead, Metaverse Governance

Metaverse Initiative Project Fellows

Kevin Collins

Managing Director, Software and Platforms, Global, Accenture USA

Matt Price

Responsible Metaverse Strategy Manager, Metaverse Continuum Business Group (MCBG), Accenture USA

Anna Schilling

Data and AI Value Strategy Manager, Applied Intelligence Strategy, Accenture USA

David Treat

Senior Managing Director, MCBG Lead, Accenture USA

Kathryn White

Responsible Metaverse Lead, MCBG, Accenture USA

Steering Committee Members

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

Judson Althoff

Chief Commercial Officer, Microsoft

Jeremy Bailenson

Thomas More Storke Professor of Communication, Stanford University

Stephanie Burns

Senior Vice-President and General Counsel, Sony

Adam Caplan

Senior Vice-President, Emerging Technology, Salesforce

Inhyok Cha

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

Phil Chen

Chief Decentralized Officer, HTC-VIA

Nick Clegg

President, Global Affairs, Meta

Julia Goldin

Chief Product and Marketing Officer, LEGO Group

Julie Inman Grant

eSafety Commissioner, Office of the eSafety Commissioner, Australia

Marwan Bin Haidar

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

Mansoor Hanif

Head, Infrastructure Policy and Emerging Technologies, NEOM

Huda Al Hashimi

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

Brittan Heller

Fellow, Digital Forensics Research Lab, The Atlantic Council

Paula Ingabire

Minister of Information Communication Technology and Innovation, Government of Rwanda

Peggy Johnson

Chief Executive Officer, Magic Leap

Nuala O'Connor

Senior Vice-President and Chief Counsel, Digital Citizenship, Walmart

Tony Parisi

Chief Product Officer, Lamina1

Philip Rosedale

Co-Founder, High Fidelity

Yat Siu

Co-Founder and Executive Chairman, Animoca Brands

Hugo Swart

Vice-President and General Manager, XR, Qualcomm

Artur Sychov

Founder and Chief Executive Officer, Somnium Space

Kent Walker

President, Global Affairs and Chief Legal Officer, Google

Wilson White

Vice-President, Government Affairs and Public Policy, Google

Working group members

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

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

Joe Abi Akl

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

Seokhyun Elliott Ahn

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

Anju Ahuja

Vice-President, Product Strategy and Insights, CableLabs

Saeed Aldhaferi

Director, Center for Futures Studies, University of Dubai

Flavia Alves

Head, International Institutions Relations, Meta Platforms

Ahmed Saeed Abdulla Alshami

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

Maurizio Arseni

Freelance Tech Journalist

Yoni Assia

Chief Executive Officer, eToro

Frank Badalamenti

Partner, PwC Americas

Moritz Baier-Lentz

Partner, Lightspeed Venture Partners

Jeremy Bailenson

Professor, Stanford University

Avi Bar-Zeev

Founder and Chief Technology Officer, RealityPrime

Luna Bianchi

Advocacy Officer, Privacy Network

Doreen Bogdan

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

Gustavo Borges

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

Sebastien Borget

Chief Operations Officer and Co-Founder, The Sandbox

Marine Boulot

Vice-President, Public Relations and Communications, Improbable Worlds

Mahmut Boz

Head, Anticipatory Regulation and Regulatory Experimentation, NEOM

Gareth Burkhill-Howarth

Global Data Protection Officer, WPP

Jehangir Byramji

Emerging Technology and Innovation, Lloyds Banking Group

Marquis Cabrera

Chairman and Chief Executive Officer, Stat Zero

Adam Caplan

Senior Vice-President, Emerging Technology, Salesforce

Isaac Castro

Co-Chief Executive Officer and Co-Founder, Emerge

Achyut Chandra

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

Pearly Chen

Vice-President, HTC-VIA

Phil Chen

Chief Decentralization Officer, HTC-VIA

Magda Cocco

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

Anna Maria Collard

Senior Vice-President, Content Strategy and Evangelist Africa, Knowbe4 Africa

Sandra Cortesi

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

Sadie Creese

Professor of Cybersecurity, University of Oxford

William Cutler

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

Nighat Dad

Executive Director, Digital Rights Foundation

Julie Dawson

Chief Policy and Regulatory Officer, Yoti

Eileen Donahoe

Executive Director, Global Digital Policy Incubator, Stanford

Sarah Kate Ellis

President and Chief Executive Officer, GLAAD

Liv Erickson

Innovation Ecosystem Development Lead, Mozilla

Maureen Fan

Co-Founder and Chief Executive Officer, Baobab

Nita Farahany

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

Dena Feldman

Policy Director, Reality Labs, Meta Platforms

Steven Feldstein

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

Inbal Goldberger

Vice-President of Trust and Safety, ActiveFence

Paula Gomes Freire

Managing Partner, Vieira de Almeida & Associados

Patrick Grady

Policy Analyst, Center for Data Innovation

Ashraf Hamed

Value Proposition Innovation and Pioneering, SAP

Cortney Harding

Chief Executive Officer, Friends with Holograms

Susie Hargreaves

Chief Executive Officer, Internet Watch Foundation (IWF)

Huda Al Hashimi

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

Mohamed Heikal

Head, Corporate Development, Majid Al Futtaim Holding

Vera Heitmann

Leader, Digital and Growth, Public Affairs, IKEA

Brittan Heller

Fellow, The Atlantic Council

Heidi Holman

Assistant General Counsel, Microsoft

Elizabeth Hyman

Chief Executive Officer, XR Association

Tatsuya Ichikawa

Chief Executive Officer, Avers

Stephanie Ifayemi

Global Shaper, London Hub

Rolf Illenberger

Managing Director, VRdirect

Michael Jacobides

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

Mikaela Jade

Founder and Chief Executive Officer, Indigital

Amy Jordan

Director, Technology Policy, Office of Communications (Ofcom)

Makarand Joshi

Director, Strategy, Innovation and Standards, Schneider Electric

Tony Justman

Vice-President and Deputy General Counsel, Sony Interactive Entertainment

Lea Kaspar

Executive Director, Global Partners Digital

Stephen Kavanagh

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

Masa Kawashima

Executive Producer, Director of Asia Pacific Operations, Niantic

Hoda Al Khzaimi

Assistant Research Professor, New York University, Abu Dhabi

Melissa Kiehl

Innovation Adviser, XR, ICRC

Ingrid Kopp

Co-Founder, Electric South

Ashish Kumar

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

Fabio La Franca

Founding Partner, Blueverse Ventures

Natalie Lacey

Executive Vice-President, Ipsos Media, Ipsos

Martina Larkin

Chief Executive Officer, Project Liberty

Su Kiang Lau

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

Helena Leurent

Director-General, Consumers International

Stephanie Llamas

Principal, Metaverse Foresight Strategy, VoxPop Insights

Leon Lyu

Co-Founder, Booming Tech

Kuniyoshi Mabuchi

Managing Director, PwC Japan

Deena Magnall

Director, Global Digital and Technology Policy, L'Oréal

Noora Al Malek

Associate Project Manager, Artificial Intelligence Office, United Arab Emirates Government

Charles de Marcilly

Administrator, Council of the European Union

Eva Maydell

Member, European Parliament

Dinusha Mendis

Professor of Intellectual Property and Innovation Law, Bournemouth University

Jade Meskill

Vice-President, Product, Magic Leap

Mauro Miedico

Deputy Director and Chief, Special Projects and Innovation, United Nations Office on Counter Terrorism (UNOCT)

Anna Miyagi

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

Hiroaki Miyata

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

Hamdullah Mohib

Managing Director, Khas Fund, Chimera Investment

Ahram Moon

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

Steve Morris

International Chair, Portland Communications, Omnicom

Angelica Munson

Executive Officer, Chief Digital Officer, Shiseido

Eli Noam

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

Madan Oberoi

Executive Director, Technology and Innovation, INTERPOL

Genki Oda

Chairman and Chief Executive Officer, Remixpoint

Reinhard Oertli

Partner, Zurich, MLL Meyerlustenberger Lachenal Froriep

Judith Okonkwo

Founder, Imisí 3D Creation Lab

Helen Papagiannis

Founder, XR Goes Pop

Charles Paré

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

Park Yuhyun

Founder and Chief Executive Officer, DQ Institute

Erin Marie Parsons

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

Kavya Pearlman

Founder and Chief Executive Officer, XR Safety Initiative

Amy Peck

Founder and Chief Executive Officer, EndeavorXR

Bertrand Perez

Chief Executive Officer, Web 3.0 Technologies Foundation

Susan Persky

Head, Immersive Simulation Program; Head, Health Communication and Behavior Unit, National Human Genome Research Institute (NHGRI), The National Human Genome Research Institute

David Ryan Polgar

Founder and Executive Director, All Tech is Human

Nicola Port

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

Saif Al Rahma

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

Yonatan Raz-Fridman

Founder and Chief Executive Officer, Supersocial

Simmy Rease

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

Michaël Reffay

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

Gina Reif Ilardi

General Counsel, Vindex

Dan Rice

Vice-President, Digital Governance, Walmart

Tim Roberts

Managing Director, AlixPartners

Katitza Rodriguez

International Rights Director, Electronic Frontier Foundation (EFF)

Philip Rosedale

Co-Founder, High Fidelity

Sarah Sakha

Public Policy Manager, Meta Platforms

Erica Salinas

Principal Tech Leader, Web3, Amazon

Var Shankar

Director, Policy, Responsible Artificial Intelligence Institute

Nagwa El Shenawi

Undersecretary, Ministry of Communications and Information Technology of Egypt

Lewis Smithingham

Director, Creative Solutions, S4Capital

Sly Spencer-Lee

Co-Chief Executive Officer and Co-Founder, Emerge

Ian Stevenson

Chief Executive Officer, Cyacomb

Philippe Stransky-Heilkron

Senior Vice-President and Chief Architect, Kudelski

Artur Sychov

Founder and Chief Executive Officer, Somnium Space

Claire Thwaites

Senior Director EMEA Government Affairs, The LEGO Group

Timmu Toke

Chief Executive Officer and Founder, Wolfprint 3D

Neil Trevett

President, Metaverse Standards Forum

Paul Trueman

Senior Vice-President, Cyber and Intelligence Solutions, Mastercard

Matthew Vick

Deputy Director, Futures and Innovation, HM Revenue and Customs

Steven Vosloo

Digital Policy Specialist, UNICEF

Larry Wade

Senior Director, Crypto/BC Risk and Compliance, PayPal

Kent Walker

President, Global Affairs and Chief Legal Officer, Google

Lynette Wallworth

Artist, Studio Wallworth

Alice Wang

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

Gregory Welch

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

Deborah Welsh

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

Josh Williams

Chief Executive Officer, Forte

Jonathan Wong

Group President, Group ONE Holdings

Samer Yaghnam

Chief Legal and Administrative Officer, Olayan

Yu Yuan

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

Robby Yung

Chief Executive Officer, Animoca Brands

Erez Zaionce

Director, Centre for the Fourth Industrial Revolution Colombia

Production

Laurence Denmark

Creative Director, Studio Miko

Sophie Ebbage

Designer, Studio Miko

Martha Howlett

Editor, Studio Miko

George Messer

Designer, Studio Miko

Endnotes

1. ISACA, New Digital Trust Research Reveals Gaps, Benefits and Key Takeaways for Future Digital Transformations [Press release], 15 September 2022, <https://www.isaca.org/why-isaca/about-us/newsroom/press-releases/2022/new-digital-trust-research-reveals-gaps-benefits-and-key-takeaways>.
2. World Economic Forum, *Earning Digital Trust: Decision-Making for Trustworthy Technologies*, 2022, https://www3.weforum.org/docs/WEF_Earning_Digital_Trust_2022.pdf.
3. “Universal Declaration of Human Rights”, *United Nations*, 1948, <https://www.un.org/en/about-us/universal-declaration-of-human-rights>.
4. United Nations, *Guiding Principles on Business and Human Rights*, 2011, https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf.
5. World Economic Forum, *Global Principles on Digital Safety: Translating International Human Rights for the Digital Context*, 2023, <https://www.weforum.org/whitepapers/global-principles-on-digital-safety-translating-international-human-rights-for-the-digital-context/>.
6. “Article 12 of the Universal Declaration of Human Rights”, *United Nations*, 1948, <https://www.un.org/en/about-us/universal-declaration-of-human-rights>.
7. “Responsible innovation”, *UK Research and Innovation*, 10 May 2023, <https://www.ukri.org/about-us/policies-standards-and-data/good-research-resource-hub/responsible-innovation/#:~:text=For%20researchers%2C%20responsible%20innovation%20is,consequences>.
8. Price, Matthew, “Part 1: From Human-Centric Design to Human-First Design in the Metaverse”, *Medium*, 3 April 2023, <https://medium.com/@matthewpricephd/part-1-from-human-centric-design-to-human-first-design-in-the-metaverse-bad99598488a>.
9. Neo, Jun Rong Jeffery, Andrea Stevenson Won and Mardelle McKuskey Shepley, “Designing Immersive Virtual Environments for Human Behavior Research”, *Frontiers in Virtual Reality*, vol. 2, 2021, <https://doi.org/10.3389/frvir.2021.603750>.
10. Radoff, John, “The Experiences of the Metaverse”, *Medium*, 27 May 2021, <https://medium.com/building-the-metaverse/the-experiences-of-the-metaverse-2126a7899020>.
11. “What does privacy mean?”, *iapp*, n.d., <https://iapp.org/about/what-is-privacy/>.
12. “SAFETY Definition & Legal Meaning”, *The Law Dictionary*, n.d., <https://thelawdictionary.org/safety/>.
13. “Digital Trust”, *World Economic Forum*, n.d., <https://initiatives.weforum.org/digital-trust/about>.
14. “Promoting well-being”, *World Health Organization*, n.d., <https://www.who.int/activities/promoting-well-being>.
15. “Building a Responsible Metaverse”, *Accenture*, 10 February 2023, <https://www.accenture.com/us-en/insights/technology/responsible-metaverse>.
16. Bodó, Balázs, Jaya Klara Brekke and Jaap-Henk Hoepman, “Decentralisation: a multidisciplinary perspective”, *Internet Policy Review*, vol. 10, issue 2, 2022, <https://policyreview.info/concepts/decentralisation>.
17. Rice, Tatiana, “When is a Biometric No Longer a Biometric?”, *Future of Privacy Forum*, 19 May 2022, <https://fpf.org/blog/when-is-a-biometric-no-longer-a-biometric/>.
18. Federal Register, *Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses*, *Federal Register Notice 86*, 2022, <https://www.ai.gov/rfi/2022/86-FR-56300/XR-Safety-Initiative-Biometric-RFI-2022.pdf>.
19. World Economic Forum, *Interoperability in the Metaverse*, 2023, https://www3.weforum.org/docs/WEF_Interoperability_in_the_Metaverse.pdf.
20. Renieris, Elizabeth M., *Beyond Data: Reclaiming Human Rights at the Dawn of the Metaverse*, The MIT Press, 2023.
21. “What constitutes data processing?”, *European Commission*, n.d., https://commission.europa.eu/law/law-topic/data-protection/reform/what-constitutes-data-processing_en.
22. “International standards: Special Rapporteur on the right to privacy”, *United Nations*, n.d., <https://www.ohchr.org/en/special-procedures/sr-privacy/international-standards>.
23. Livingstone, Sonia and Kruakae Pothong, “Child Rights by Design: our guidance for innovators toolkit is finally here!”, *Digital Futures Commission Blog*, 31 March 2023, <https://digitalfuturescommission.org.uk/blog/child-rights-by-design-our-guidance-for-innovators-toolkit-is-finally-here/>.
24. “UN Declaration on the Rights of Indigenous Peoples”, *United Nations*, 13 September 2007, <https://www.ohchr.org/en/indigenous-peoples/un-declaration-rights-indigenous-peoples>.
25. Greenfield, Emma, “Digital Equity for Indigenous Communities”, *Samuel Centre for Social Connectedness*, 7 July 2020, <https://www.socialconnectedness.org/digital-equity-for-indigenous-communities/>.
26. Lin, Jinghuai and Latoschik, Marc Erich, “Digital body, identity and privacy in social virtual reality: A systematic review”, *Frontiers in Virtual Reality*, vol. 3, 2022, <https://www.frontiersin.org/articles/10.3389/frvir.2022.974652/full>.
27. Ramos, Andy, “The metaverse, NFTs and IP rights: to regulate or not to regulate?”, *WIPO Magazine*, June 2022, https://www.wipo.int/wipo_magazine/en/2022/02/article_0002.html.
28. “Intellectual Property in the Metaverse. Episode IV: Copyright”, *European Innovation Council and SMEs Executive Agency*, 30 June 2022, https://intellectual-property-helpdesk.ec.europa.eu/news-events/news/intellectual-property-metaverse-episode-iv-copyright-2022-06-30_en.

29. “The Future of Metaverse and Our Brain: Science, Technology, and Ethics”, *Frontiers in Medical Technology*, 2023, <https://www.frontiersin.org/research-topics/43750/the-future-metaverse-and-our-brain-science-technology-and-ethics>.
30. Guzman H., Lorena, “Chile: Pioneering the protection of neurorights”, *The UNESCO Courier*, 2022, <https://en.unesco.org/courier/2022-1/chile-pioneering-protection-neurorights>.
31. Regulatory Horizons Council, *Neurotechnology Regulation*, 2022, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1135956/rhc-neurotechnology-regulation.pdf.
32. Borbón, Diego and Borbón, Luisa, “A Critical Perspective on NeuroRights: Comments Regarding Ethics and Law”, *Frontiers in Human Neuroscience*, vol. 15, 2021, <https://www.frontiersin.org/articles/10.3389/fnhum.2021.703121/full>.
33. Rosenberg, Louis, “Marketing in the Metaverse and the need for Consumer Protections”, *2022 IEEE 13th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, 2022, pp. 35-39, <https://ieeexplore.ieee.org/document/9965661>.
34. “INTERPOL launches first global police Metaverse”, *INTERPOL*, 20 October 2022, <https://www.interpol.int/en/News-and-Events/News/2022/INTERPOL-launches-first-global-police-Metaverse>.
35. “Global Coalition for Digital Safety”, *World Economic Forum*, <https://initiatives.weforum.org/global-coalition-for-digital-safety/about>.
36. “Meet your new AI colleague; Indiana University Kelley School of Business professor studies working with digital humans”, *News Wise*, 15 February 2023, <https://www.newswise.com/articles/meet-your-new-ai-colleague-iu-kelley-school-of-business-professor-studies-working-with-digital-humans>.
37. Syemour, Mike and Lovallo, Dan and Riemer, Kai and Dennis, Alan R. and Yuan, Lingyao (Ivy), “AI with a Human Face”, *Harvard Business Review*, March-April 2023, <https://hbr.org/2023/03/ai-with-a-human-face>.
38. Hinduja, Sameer, “The Metaverse: Opportunities, Risks, and Harms”, *Cyberbullying Research Center*, n.d., <https://cyberbullying.org/metaverse>.
39. UNICEF, *Legislating for the digital age: Global guide on improving legislative frameworks to protect children from online sexual exploitation and abuse*, 2022, <https://www.unicef.org/media/120386/file/Legislating%20for%20the%20digital%20age%20Global%20Guide.pdf>.
40. Zubernis, Lynn, “Can Social Media and Online Communities Be Good for Us?”, *Psychology Today*, 28 March 2023, <https://www.psychologytoday.com/us/blog/the-science-of-fandom/202303/can-social-media-and-online-communities-be-good-for-us>.
41. Anderson, Janna and Lee Rainie, “Stories from Experts About the Impact of Digital Life: 2. The negatives of digital life”, *Pew Research Center*, 3 July 2018, <https://www.pewresearch.org/internet/2018/07/03/the-negatives-of-digital-life/>.
42. “Data Privacy Vs. Data Protection: Understanding The Distinction In Defending Your Data”, *Forbes*, 19 December 2018, <https://www.forbes.com/sites/forbestechcouncil/2018/12/19/data-privacy-vs-data-protection-understanding-the-distinction-in-defending-your-data/?sh=5845e77750c9>.
43. Nair, Vivek, Gonzalo Garrido and Dawn Song, *Exploring the Unprecedented Privacy Risks of the Metaverse*, 2022, <https://arxiv.org/pdf/2207.13176.pdf>.
44. Scott, Anna, Jack Hardinges and Jeni Tennison, “Explainer: What is personal data and how can I control how it’s shared?”, *Open Data Institute*, 6 April 2018, <https://www.theodi.org/article/explainer-what-is-personal-data-and-how-can-i-control-how-is-it-shared/>.
45. Samson, Renate, Kayshani Gibbon and Anna Scott, *About Data About Us*, Open Data Institute, Luminate, RSA, 2019, <https://www.thersa.org/globalassets/pdfs/reports/data-about-us-final-report.pdf>.
46. Rice, Tatiana, “When is a Biometric No Longer a Biometric?”, *Future of Privacy Forum*, 19 May 2022, <https://fpf.org/blog/when-is-a-biometric-no-longer-a-biometric/>.
47. “Biometric data”, *XRSI*, n.d., <https://xrsi.org/definition/biometric-data>.
48. “Biometrics”, *NIST*, n.d., <https://csrc.nist.gov/glossary/term/biometrics>.
49. “Geospatial Data”, *XRSI*, n.d., <https://xrsi.org/definition/geospatial-data>.
50. “psychographics”, *Oxford Reference*, n.d., <https://www.oxfordreference.com/display/10.1093/acref/9780199568758.001.0001/acref-9780199568758-e-2187>.
51. World Economic Forum, *The Internet of Bodies Is Here: Tackling new challenges of technology governance*, 2020, <https://www.weforum.org/reports/the-internet-of-bodies-is-here-tackling-new-challenges-of-technology-governance>.
52. “sensitive information”, *NIST*, n.d., <https://csrc.nist.gov/glossary/term/sensitive-information>.
53. “Personal Information”, *NIST*, n.d., <https://csrc.nist.gov/glossary/term/personal-information>.
54. “Personal Data Protection and Privacy”, *UN System Chief Executives Board for Coordination*, n.d., <https://unsceb.org/privacy-principles>.
55. “What is PHI?”, *US Department of Health and Human Services*, n.d., <https://www.hhs.gov/answers/hipaa/what-is-phi/index.html>.
56. European Parliament, *Metaverse Opportunities, risks and policy implication*, 2022, [https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733557/EPRS_BRI\(2022\)733557_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733557/EPRS_BRI(2022)733557_EN.pdf).

57. Heller, Brittan, “Watching Androids Dream of Electric Sheep: Immersive Technology, Biometric Psycography, and the Law”, *Vanderbilt Journal of Entertainment and Technology Law*, vol. 23, issue 1, 2021, <https://scholarship.law.vanderbilt.edu/jetlaw/vol23/iss1/1/>.
58. Wrabetz, Joan, “What is Inferred Data and Why Is It Important?”, *Business Law Today*, 22 August 2022, <https://businesslawtoday.org/2022/08/what-is-inferred-data-why-is-it-important/>.
59. “What does data protection ‘by design’ and ‘by default’ mean?”, *European Commission*, n.d., https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en.
60. “A guide to lawful basis”, *Information Commissioner’s Office*, n.d., <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/>.
61. Cory, Nigel and Luke Dascoli, “How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them”, *Information Technology & Innovation Foundation*, 19 July 2021, <https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/>.
62. World Economic Forum, *A Roadmap for Cross-Border Data Flows: Future-Proofing Readiness and Cooperation in the New Data Economy*, 2020, https://www3.weforum.org/docs/WEF_A_Roadmap_for_Cross_Border_Data_Flows_2020.pdf.
63. “What is personal information: a guide”, *Information Commissioner’s Office*, n.d., <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/personal-information-what-is-it/what-is-personal-information-a-guide/>.
64. Nair, Vivek, Wenbo Guo, Jutus Mattern, Rui Wang, James F. O’Brien, Louis Rosenberg and Dawn Song, “Unique Identification of 50,000+ Virtual Reality Users from Head & Hand Motion Data”, *arXiv e-prints*, 2023, <https://arxiv.org/pdf/2302.08927.pdf>.
65. Ibid.
66. World Economic Forum, *Data Free Flow with Trust: Overcoming Barriers to Cross-Border Data Flows*, 2023, <https://www.weforum.org/whitepapers/data-free-flow-with-trust-overcoming-barriers-to-cross-border-data-flows>.
67. Organisation for Economic Co-operation and Development, *The OECD Guidelines*, 2011, <https://www.oecdwatch.org/oecd-ncps/the-oecd-guidelines-for-mnes/#:~:text=The%20OECD%20Guidelines%20for%20Multinational,labour%20rights%2C%20and%20the%20environment>.
68. “Privacy Enhancing Technologies”, *The Royal Society*, 23 January 2023, <https://royalsociety.org/topics-policy/projects/privacy-enhancing-technologies/>.
69. “Homomorphic Encryption Standardization”, n.d., <https://homomorphicencryption.org/introduction/>.
70. “What are zero-knowledge proofs”, *Ethereum*, 30 June 2023, <https://ethereum.org/en/zero-knowledge-proofs/>.
71. World Economic Forum, *Cyber Resilience Playbook for Public-Private Collaboration*, 2018, https://www3.weforum.org/docs/WEF_Cyber_Resilience_Playbook.pdf.
72. “Dissociative Disorders”, *National Alliance on Mental Illness*, <https://www.nami.org/About-Mental-Illness/Mental-Health-Conditions/Dissociative-Disorders>.
73. Rosbach, Molly, “Virtual reality, real injuries: OSU study shows how to reduce physical risk in VR”, *Oregon State University*, 7 January 2020, <https://today.oregonstate.edu/news/virtual-reality-real-injuries-osu-study-shows-how-reduce-physical-risk-vr>.
74. “Dissociative Disorders”, *National Alliance on Mental Illness*, <https://www.nami.org/About-Mental-Illness/Mental-Health-Conditions/Dissociative-Disorders>.
75. Chen, Wanting, Jiaqing Song, Yuwei Wang, Changxu Wu, et al., “Inattention blindness to unexpected hazard in augmented reality head-up display assisted driving: The impact of the relative position between stimulus and augmented graph”, *Traffic Injury Prevention*, vol. 24, issue 4, 2023, pp. 344-351, <https://pubmed.ncbi.nlm.nih.gov/36939683/>.
76. Blascovlch, Jim and Jeremy Ballenson, “Infinite Reality,” *Harper Collins Publishers*, 2011.
77. Rosbach, Molly, “Virtual reality, real injuries: OSU study shows how to reduce physical risk in VR”, *Oregon State University*, 7 January 2020, <https://today.oregonstate.edu/news/virtual-reality-real-injuries-osu-study-shows-how-reduce-physical-risk-vr>.
78. Bipartisan Policy Center, *Thinking Ahead About XR*, 2022, p. 20, https://bipartisanpolicy.org/download/?file=/wp-content/uploads/2022/04/XR-Report_Final-Copy.pdf.
79. Price, Matthew, “Part 1: From Human-Centric Design to Human-First Design in the Metaverse”, *Medium*, 3 April 2023, <https://medium.com/@matthewpricephd/part-1-from-human-centric-design-to-human-first-design-in-the-metaverse-bad99598488a>.
80. “A guide to lawful basis”, *Information Commissioner’s Office*, n.d., <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/>.
81. World Economic Forum, *Redesigning Data Privacy: Reimagining Notice & Consent for human-technology interaction*, 2020, https://www3.weforum.org/docs/WEF_Redesigning_Data_Privacy_Report_2020.pdf.
82. Ibid.
83. XRSI, *The XRSI Privacy and Safety Framework*, 2020, <https://xrsi.org/publication/the-xrsi-privacy-framework>.
84. “What does ‘grounds of legitimate interest’ mean?”, *European Commission*, n.d., https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/what-does-grounds-legitimate-interest-mean_en#:~:text=Your%20company%2Forganisation%20has%20a,security%20of%20your%20IT%20systems.

85. European Commission, *Commission proposes a trusted and secure Digital Identity for all Europeans* [Press release], 3 June 2021, https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2663.
86. World Economic Forum, *Advancing Digital Agency: The Power of Data Intermediaries*, 2022, https://www3.weforum.org/docs/WEF_Advancing_towards_Digital_Agency_2022.pdf.
87. West, David, “Accessing and Protecting Digital Assets: Fiduciary Duties in a Digital World”, *NextGen Financial Services Report*, 28 February 2019, <https://www.nextgenfinancialservicesreport.com/2019/02/accessing-and-protecting-digital-assets-fiduciary-duties-in-a-digital-world/#:~:text=The%20fiduciary%20is%20an%20authorized,laws%20governing%20unauthorized%20computer%20access>.
88. “Personalized Privacy Assistant”, *Carnegie Melon University: Societal Computing*, n.d., <https://sc.cs.cmu.edu/research-detail/74-personalized-privacy-assistant>.
89. Figueiredo, Carlos, “Content moderation in challenging times”, *Venture Beat*, 21 May 2020, <https://venturebeat.com/business/content-moderation-in-challenging-times/>.
90. “Responsible Design”, *Loughborough University*, n.d., <https://www.lboro.ac.uk/schools/design-creative-arts/research-innovation/our-research/responsible-design/#:~:text=Achieving%20balanced%20social%2C%20environmental%20and,inclusive%20and%20sustainable%20design%20practice>.
91. Accenture, *From AI compliance to competitive advantage*, 2022, https://www.accenture.com/us-en/insights/artificial-intelligence/ai-compliance-competitive-advantage?c=acn_glbbrandexpressiongoogle_13201901&n=psgs_0822&gclid=CjwKCAiA3KefBhByEiwAi2LDHJqxsSpbZeATRNjkuTNCcZ8mXTsmGsUOXqk3rWk8_wZ6jQMIB5o-BoCvXMQAvD_BwE&gclidsrc=aw.ds.
92. Krishnamurthy, Prabhakar, “Understanding Data Bias: Types and sources of data bias”, *Medium*, 11 September 2019, <https://towardsdatascience.com/survey-d4f168791e57>.
93. Lee, Nicol, Paul Resnick and Genie Barton, *Algorithmic bias detection and mitigation: Best practices and policies to reduce consumer harms*, Brookings, 2019, <https://www.brookings.edu/research/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/>.
94. “European Centre for Algorithmic Transparency”, *European Commission*, n.d., https://algorithmic-transparency.ec.europa.eu/index_en.
95. Gryz, Jarek and Marcin Rojszczak, “Black box algorithms and the rights of individuals: no easy solution to the “explainability” problem”, *Internet Policy Review*, vol. 10, issue 2, 2021, <https://policyreview.info/articles/analysis/black-box-algorithms-and-rights-individuals-no-easy-solution-explainability>.
96. “Offboarding definition”, *Law Insider*, n.d., <https://www.lawinsider.com/dictionary/offboarding>.
97. Coulson, M., A. Oskis, R. Spencer and R. Gould, “Tourism, migration, and the exodus to virtual worlds: Place attachment in massively multiplayer online gamers.”, *Psychology of Popular Media*, vol. 9, issue 4, 2020, <https://psycnet.apa.org/doiLanding?doi=10.1037%2Fppm0000244>.
98. Smith, Noah, “Racism, misogyny, death threats: Why can’t the booming video-game industry curb toxicity?”, *The Washington Post*, 26 February 2019, <https://www.washingtonpost.com/technology/2019/02/26/racism-misogyny-death-threats-why-cant-booming-video-game-industry-curb-toxicity/>.
99. Ibid.
100. “Consent to use data on children”, *European Union Agency on Fundamental Rights (FRA)*, n.d., <http://fra.europa.eu/en/publication/2017/mapping-minimum-age-requirements-concerning-rights-child-eu/consent-use-data-children>.
101. United Nations, *Convention on the Rights of the Child*, 1989, <https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child>.
102. “The LEGO Group and Epic Games team up to build a place for kids to play in the metaverse”, *Lego*, 7 April 2022, <https://www.lego.com/en-us/aboutus/news/2022/april/the-lego-group-and-epic-games-team-up-to-build-a-place-for-kids-to-play-in-the-metaverse?locale=en-us>.
103. Sanctuary, Hillary, “Virtual reality affects children differently than adults”, *SciencyDaily*, 27 September 2021, <https://www.sciencedaily.com/releases/2021/09/210927092144.htm>.
104. Ryokai, Kimiko, Sandra Jacobo, Edward Rivero and Julia Park, “Examining children’s design processes, perspective-taking, and collaboration when using VR head-mounted displays”, *International Journal of Child-Computer Interaction*, vol. 33, 2022, <https://www.sciencedirect.com/science/article/abs/pii/S2212868921001227>.
105. “Consent to use data on children”, *European Union Agency on Fundamental Rights (FRA)*, n.d., <http://fra.europa.eu/en/publication/2017/mapping-minimum-age-requirements-concerning-rights-child-eu/consent-use-data-children>.
106. Montgomery, Elaine and Elaina Koros, “Meta’s Best Interests of the Child Framework”, *TTC Labs*, n.d., <https://www.ttclabs.net/news/metas-best-interests-of-the-child-framework#:~:text=The%20UNCRC%20emphasizes%20that%20in,an%20important%20principle%20in%20product>.
107. “General comment No. 25 (2021) on children’s rights in relation to the digital environment”, *United Nations*, 2 March 2021, <https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation>.
108. UNICEF, *The Case for Better Governance of Children’s Data: A Manifesto*, 2021, <https://www.unicef.org/globalinsight/media/1741/file/UNICEF%20Global%20Insight%20Data%20Governance%20Manifesto.pdf>.
109. United Nations, *Convention on the Rights of the Child*, 1989, <https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child>.

110. “guardian”, *Legal Dictionary*, n.d., <https://dictionary.law.com/Default.aspx?selected=843>.

111. “Child Assent”, *LawDistrict*, n.d., <https://www.lawdistrict.com/legal-dictionary/child-assent>.

112. “Digital literacy for children – 10 things to know”, *UNICEF*, n.d., <https://www.unicef.org/globalinsight/documents/digital-literacy-children-10-things-know#:~:text=Digital%20literacy%20goes%20beyond%20technical,and%20learning%20through%20digital%20technologies>.

113. “DigComp”, *European Commission*, n.d., [https://joint-research-centre.ec.europa.eu/digcomp_en#:~:text=The%20integrated%20DigComp%202.2%20framework,by%20artificial%20intelligence%20\(AI\)](https://joint-research-centre.ec.europa.eu/digcomp_en#:~:text=The%20integrated%20DigComp%202.2%20framework,by%20artificial%20intelligence%20(AI))

114. Code of Federal Regulations, *Part 312 – Children’s Online Privacy Protection Rule*, 2013, <https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312>.

115. “What should our general approach to processing children’s personal data be?”, *Information Commissioner’s Office*, n.d., <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/children-and-the-uk-gdpr/what-should-our-general-approach-to-processing-children-s-personal-data-be/>.

116. Vosloo, Steven, “EU Digital Services Act: How it will make the internet safer for children”, *World Economic Forum*, 20 June 2022, <https://www.weforum.org/agenda/2022/06/eu-digital-service-act-how-it-will-safeguard-children-online/>.

117. “A guide to the Online Safety Bill”, *GOV.UK*, 16 December 2022, <https://www.gov.uk/guidance/a-guide-to-the-online-safety-bill#how-the-online-safety-bill-will-protect-children>.

118. “The Children’s code design guidance”, *Information Commissioner’s Office*, n.d., <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/digital-design/childrens-code-design-guidance/>.

119. “Introduction to the Children’s code”, *Information Commissioner’s Office*, n.d., <https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-code/>.

120. “The Child Safety Initiative”, *XRSI*, n.d., <https://xrsi.org/programs/child-safety>.

121. Umbach, Christian, “How to accelerate digital literacy in the enterprise world”, *World Economic Forum*, 5 February 2020, <https://www.weforum.org/agenda/2020/02/accelerating-digital-literacy-in-the-enterprise-world/>.

122. Trautman, Stephanie, “5 ways we can develop the digital skills our economy needs”, *World Economic Forum*, 16 January 2023 <https://www.weforum.org/agenda/2023/01/5-ways-develop-digital-skills-davos2023/>.

123. XRSI, “Day 1 – Human Rights in the Metaverse | 10th December”, *Youtube*, 10 December 2022, <https://www.youtube.com/watch?v=u1ELh5hxxXU>.

124. Norton Rose Fullbright, *The Metaverse: The evolution of a universal digital platform*, 2021, <https://www.nortonrosefulbright.com/de-de/wissen/publications/5cd471a1/the-metaverse-the-evolution-of-a-universal-digital-platform#section1>.

125. “Into the Digital World: XRA’s Guide to Immersive Technology”, *XR Association*, n.d., <https://xra.org/howxrworks/>.

126. “Online Safety”, *US Department of Homeland Security*, n.d., <https://www.dhs.gov/blue-campaign/online-safety>.

127. “The Cyber Threat”, *Federal Bureau of Investigation (FBI)*, n.d., <https://www.fbi.gov/investigate/cyber>.

128. “Common Scams and Crimes”, *Federal Bureau of Investigation (FBI)*, n.d., <https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes>.

129. “XRA’s Developers Guide, Chapter 1: Fundamental Design Principles for Immersive Experiences”, *XR Association*, October 2018, <https://xra.org/research/xr-primer-1-0-a-starter-guide-for-developers/>.

130. “XRA’s Developers Guide, Chapter 3: Accessibility & Inclusive Design in Immersive Experiences”, *XR Association*, October 2018, <https://xra.org/research/xra-developers-guide-accessibility-and-inclusive-design/>.

“XRA’s Developers Guide, Chapter 2: Creating Safe, Inclusive, and Respectful Immersive Experiences”, *XR Association*, October 2018, <https://xra.org/research/xr-primer-2-0-a-starter-guide-for-developers/>.

131. “XRA’s Developers Guide, Chapter 4: Designing Immersive Learning for Secondary Education”, *XR Association*, October 2018, <https://xra.org/research/xras-developers-guide-chapter-four-designing-immersive-learning-for-secondary-education/>.

132. Smeets, Martin (ed.), “Chapter 16: Converging thoughts on digital trade in preparing for the future”, in *Adapting to the Digital Trade Era: Challenges and opportunities*, pp. 335-347, *World Trade Organization Publications*, 2021, https://www.wto.org/english/res_e/booksp_e/adtera_e.pdf.

133. *World Trade Organization*, *World Trade Report 2018: The future of world trade: How digital technologies are transforming digital commerce*, 2018, https://www.wto.org/english/res_e/publications_e/world_trade_report18_e.pdf.

134. Davis, Wynne, “What Is StockX And Why Is Nike Suing Them?”, *NPR*, 12 May 2022, <https://www.npr.org/2022/05/12/1098426367/stockx-nike-lawsuit-sneakers>.

135. Feitelber, Rosemary, “Hermès Wins Lawsuit Against Mason Rothschild Over ‘MetaBirkins’ NFTs”, *Women’s Wear Daily (WWD)*, 8 February 2023, <https://wwd.com/fashion-news/designer-luxury/hermes-wins-court-battle-over-metabirkins-nfts-mason-rothschild-1235510445/>.

136. “AI: The driving force behind the metaverse?”, *ITU*, 30 June 2022, <https://www.itu.int/hub/2022/06/ai-driving-force-metaverse/>.

137. Routley, Nick, “What is generative AI? An AI explains”, *World Economic Forum*, 6 February 2023, <https://www.weforum.org/agenda/2023/02/generative-ai-explain-algorithms-work/>.
138. Kashettar, Swathi, “ChatGPT’s Vision for the Future of Metaverse”, *Analytics Insight*, 8 February 2023, <https://www.analyticsinsight.net/chatgpts-vision-for-the-future-of-metaverse/>.
139. Radoff, Jon, “Market Map: Generative AI for Virtual Worlds”, *Medium*, 2 February 2023, <https://medium.com/building-the-metaverse/market-map-generative-ai-for-virtual-worlds-efde3984e538>.
140. Takahashi, Dean, “How generative AI could create assets for the metaverse | Jensen Huang”, *GamesBeat*, 28 November 2022, <https://venturebeat.com/games/how-generative-ai-could-create-assets-for-the-metaverse-jensen-huang/>.
141. O’Connor, Ryan, “Emergent Abilities of Large Language Models”, *AssemblyAI*, 7 March 2023, <https://www.assemblyai.com/blog/emergent-abilities-of-large-language-models/>.
142. Neto, Jose, “ChatGPT and the Generative AI Hallucinations”, *Medium*, 15 March 2023, <https://medium.com/chatgpt-learning/chatgtp-and-the-generative-ai-hallucinations-62feddc72369>.
143. Wang, Yau-Shian and Yingshan Chang, “Toxicity Detection with Generative Prompt-based Inference”, *arXiv*, 2022, <https://arxiv.org/abs/2205.12390>.
144. “It doesn’t take much to make machine-learning algorithms go away”, *The Economist*, 8 April 2023, <https://www.economist.com/science-and-technology/2023/04/05/it-doesnt-take-much-to-make-machine-learning-algorithms-go-awry>.
145. Mukherjee, Supantha, Foo Yun Chee and Martin Coulter, “EU proposes new copyright rules for generative AI”, *Reuters*, 28 April 2023, <https://www.reuters.com/technology/eu-lawmakers-committee-reaches-deal-artificial-intelligence-act-2023-04-27/>.
146. Appel, Gil, Juliana Neelbauer and David Schweidel, “Generative AI Has An Intellectual Property Problem”, *Harvard Business Review*, 7 April 2023, <https://hbr.org/2023/04/generative-ai-has-an-intellectual-property-problem>.
147. Wolfewicz, Arne, “Human-in-the-Loop in Machine Learning: What is it and How Does it Work?”, *Levity*, 16 November 2022, <https://levity.ai/blog/human-in-the-loop#:~:text=Human%2Din%2Dthe%2DLoop%20aims%20to%20achieve%20what%20neither,of%20a%20continuous%20feedback%20loop>.
148. “AI ethics & governance”, *Accenture*, n.d., <https://www.accenture.com/us-en/services/applied-intelligence/ai-ethics-governance>
149. World Economic Forum, *A Blueprint for Equity and Inclusion in Artificial Intelligence*, 2022, <https://www.weforum.org/whitepapers/a-blueprint-for-equity-and-inclusion-in-artificial-intelligence/>.