SUGGESTIONS FOR THE TRAI 5G POLICY PERTAINING TO QUESTIONS ABOUT THE METAVERSE & WEB3 TECHNOLOGY BY COLOURS OF INDIA & PANDA LAW

Q.16. What are the policy measures required to create awareness and promote use of Metaverse, so that the citizens including those residing in rural and remote areas may benefit from the Metaverse use cases and services to create new economic activities and increase employment opportunities and thereby promote economic growth of the country?

The metaverse is a story of interdisciplinary intersections and combinatorial effects. As rightly noted by the Consultation Paper under reply, the metaverse, sits at the crossroads of three other emerging technologies :

A) Blockchain (Web3);
B) Artificial Intelligence/ Machine Learning
C) Augmented Reality/ Virtual Reality/ Mixed Reality

Thus, any attempt to promote the growth and development of the metaverse, would necessarily entail the promotion of all these three base technologies and ensuring that citizens, including those in rural and remote areas, can benefit from it economically, culturally and socially involves a multi-pronged approach, which we posit to be a thoughtful combination of ***a)*** regulatory measures, ***b)*** education and engagement, ***c)*** hardware and infrastructure development, ***d)*** public, private and civic society partnerships.

1. **Establishing a regulatory framework**:

a) The advent of the Metaverse heralds a new frontier that demands regulatory foresight, particularly in extending its reach to rural and remote India. Cutting-edge technologies like 5G and renewable energy sources are prerequisites, but the linchpin lies in crafting a legal framework that is both protective and enabling. This necessitates a multidisciplinary approach, incorporating insights from legal experts, technologists, and policymakers. Legal Design[1], a methodology rooted in design thinking, offers a fresh lens to tackle the complexities of this digital simulacra. By doing so, the government can lay the groundwork for an industry that is not only

[1] https://law.stanford.edu/organizations/pages/legal-design-lab/

compliant with international norms but also adaptable to the unique challenges posed by the Metaverse.

b) Trust and human dimensions emerge as the dual pillars upon which this regulatory framework must be built. Trust encompasses elements like privacy, security, and intellectual property rights, while human dimensions focus on safety, sustainability, and inclusivity. These considerations are not mere add-ons; they are integral to fostering a Metaverse that is economically viable and socially responsible. By embedding these principles into law, the government can catalyze economic activity in rural areas, where the Metaverse can serve as a platform for local entrepreneurship, education, and public services.

c) User-centricity must be the cornerstone of this regulatory endeavor. The Metaverse's inhabitants seek control over their data, an authentic yet secure digital identity, a say in the governance of the platforms, and a balanced virtual-physical existence. Meeting these demands is not just an ethical imperative but also a commercial one; a Metaverse that respects user autonomy and well-being is more likely to gain widespread acceptance. Therefore, regulations should not merely impose constraints but should empower users to engage with the Metaverse in a manner that enriches both their digital and physical lives.

d) **Encouraging investment**: Policymakers can encourage investment in the Metaverse by providing incentives for businesses and individuals to invest in Metaverse use cases and services. This can help create new economic activities and increase employment opportunities, particularly in rural and remote areas.

e) **Ensuring equitable access:** Policymakers can ensure equitable access to the Metaverse by providing funding for the development of hardware and software that is accessible to all users. This can help ensure that all citizens, regardless of their location or socioeconomic status, have access to the economic opportunities provided by the Metaverse.[2]

f) **Fostering innovation:** Policymakers can foster innovation in the Metaverse by providing funding for research and development of new Metaverse use cases and services. This can help create new economic activities and increase employment opportunities, particularly in rural and remote areas.[3]

[2] https://itif.org/publications/2021/11/15/public-policy-metaverse-key-takeaways-2021-arvr-policy-conference/
[3] https://www.brookings.edu/articles/metaverse-economics-part-1-creating-value-in-the-metaverse/

g) **Addressing potential downsides:** Policymakers can address potential downsides of the Metaverse, such as cyberbullying, misinformation, and child exploitation, by establishing regulations that protect users and ensure that the Metaverse is a safe and inclusive space for all.[4]

h) **Establishing technical standards**: Policymakers can establish technical standards for the Metaverse that ensure interoperability and portability across different platforms. This can help ensure that users can move freely between different Metaverse platforms and that the Metaverse is built on a foundation of open standards.

i) Positive messaging for Virtual Digital Assets (VDAs): As noted above, crypto-tokens/ VDAs will be a necessary building block of the metaverse stack. In the current regulatory climate, VDAs usage is perceived to be discouraged by the Government of India ("**GOI**"), mostly owing to the tax regime VDAs have been placed under where it is taxed like lottery or gambling rewards. If this public perception sustains, it may set the adoption of the metaverse back significantly.

2. Education, Awareness and Engagement:

a) To instigate Metaverse adoption in rural India, a tripartite educational formula fusing infrastructure development and community outreach with education and raising awareness is proposed.

b) First, "Metaverse Hubs" should act as foundational gateways akin to STD booths and cybercafes of the early days. These hubs must be affordable and equipped with not only high-end technology but also knowledgeable facilitators. Government intervention, through subsidies and public-private partnerships, stands as a sine qua non for this infrastructural outlay. The involvement of private companies can not only defray costs but contribute technical acumen, an indispensable advantage when navigating uncharted waters like the Metaverse.

c) Second, a robust educational strategy is needed that pairs technical training with an emphasis on immediate economic gains. A standardized curriculum, delivered at the hubs and possibly integrated into existing educational systems, will impart

[4]https://www.weforum.org/agenda/2022/05/how-to-build-an-economically-viable-inclusive-and-safe-metaverse/

both the know-how and the why-to. This curriculum must be comprehensive, covering the Metaverse's potential in specific sectors such as agriculture, healthcare, and local commerce, while also highlighting the ethical contours—data privacy, digital footprints, and responsible online behavior.

d) Finally, any effort devoid of community engagement risks falling into the chasm of irrelevance. Community-driven workshops and seminars should be intrinsic to the hubs. Gamification, which turns learning and adoption into a competitive yet communal activity, can accelerate engagement. But even as we push for rapid adoption, feedback loops must be integrated into these structures. This allows for real-time adjustments, ensuring that the initiative is not a static monolith but a responsive, evolving entity. Thus, by striking a balanced interplay among these elements, the Metaverse can be both demystified and democratized, paving the way for economic upliftment in rural and remote India.

3. Developments at the Hardware & Infrastructure Level:

a) To democratize the metaverse in rural India, one must address hardware needs beyond mere sophistication; they must be cost-effective, intuitive, and adaptable to local conditions. Mobile devices stand as the gateway, requiring advanced processors and integrated Augmented Reality ("**AR**") features. However, these high-end specifications must be reined in by affordability and power efficiency, possibly through government subsidies and optimized design. Virtual Reality ("**VR**") and AR headsets and smart glasses need to prioritize comfort, usability, and longevity, tailored to suit cultural sensibilities and climatic conditions peculiar to rural landscapes.

   As noted earlier, AR/VR devices are yet to reach mass usage. Most devices in the market place today are not quite for the mass adoption, and are prohibitively expensive. An opportunity exists to steal the lead on the designing and manufacturing of AR / VR devices in India, which if done successfully, may not only impact the device affordability but also make India a leader in different parts of the Metaverse stack.

b) In the interim, community sharing models, or easy access through the Metaverse Hubs could ease individual financial burdens, making otherwise expensive hardware like VR headsets accessible at community centers. Moreover, the devices should facilitate offline metaverse interaction, catering to bandwidth constraints.

Thus, hardware development for expanding the metaverse to rural India requires harmonizing advanced technology with ground-level practicality. Policymakers and corporations should collaborate, focusing not just on the propagation of technology but on its harmonious integration into rural life. Only through such a symbiotic relationship can the metaverse become as intrinsic to the rural fabric as it is to the urban.

c) Given the fast proliferation of satellite internet and solar power, the odds for rural and rural India connecting to the metaverse increases substantially.

d) In rural India, the leap to the metaverse is not merely a technological hurdle but a sociopolitical imperative. Ensuring its equitable reach requires a steadfast focus on two key pillars: **bandwidth** and **latency**.

   To start with bandwidth, the most straightforward solution lies in the significant scaling of infrastructure. But this is no minor undertaking. The Indian government would do well to partner with telecommunication companies to subsidize the laying down of optical fiber networks, thereby establishing high-speed internet as the new baseline. While satellite internet is also a plausible solution, its current cost model might not make it an ideal fit for low-income communities. Here, the economic viability of internet access becomes a critical part of the equation. After all, bandwidth isn't just about speed; it's about democratizing the speed at which information is accessed.

   The latency issue, though sometimes considered secondary, is just as crucial. A high-speed internet connection is less meaningful if high latency makes real-time interactions untenable. Here, edge computing shows promise. By dispersing localized data centers, possibly by utilizing existing telecommunication infrastructure, we can process data closer to its point of origin. This will not only decrease latency but also, by distributing the load, make the system more resilient to outages and disruptions.

e) The stakes transcend mere accessibility. The metaverse promises a revolution in how we think about e-commerce, education, and social interaction. However, these new regions of human endeavor will remain closed off to rural India without adequate bandwidth and low latency. Thus, the technological challenge morphs into a socio-economic one. When we prioritize bandwidth and latency, we're not merely widening access; we're advancing the cause of equality of opportunity.

4. Partnerships between the Indian government, industry and civic society:

a) To bridge the digital divide and usher the Metaverse into rural and remote India, a synergistic approach between the government and the tech industry is imperative. Existing governmental initiatives like Digital India and Skill India offer a robust foundation. These can be expanded to include Metaverse literacy, leveraging their established infrastructure to reach far-flung areas. Similarly, the Internet Saathi[5] program, a collaboration between Google and Tata Trusts, can serve as a blueprint for training "Metaverse Saathis"—women equipped to educate their communities about the Metaverse and .

b) The private sector, too, has a pivotal role. Google's Digital Unlocked[6], designed to bolster small and medium-sized businesses, can be learnt from and replicated with domestic technology companies. Furthermore, public-private partnerships can establish specialized Metaverse centers in rural areas, providing hands-on experiences and creating local ambassadors for this emerging technology. High-speed internet connectivity, facilitated by initiatives like BharatNet, will be the backbone of these endeavors, making the Metaverse accessible to the masses.

c) Lastly, community engagement must not be overlooked. Content creation challenges and grassroots digital literacy campaigns can be tailored to include Metaverse education. Events and expos focusing on digital transformation can allocate space for Metaverse technologies, offering a platform for businesses and individuals to grasp its far-reaching implications. This multi-pronged strategy ensures that the Metaverse is not just a concept confined to urban landscapes but becomes a tangible reality across India's diverse geographical and social fabric. There must also be some focus on increasing awareness as every new means of mass communication is an opportunity for the proliferation of scams and criminal activity, which has the potential to discourage large scale adoption by those stakeholders that are most at risk. Industry stakeholders may take the lead in raising awareness and educating users of the fraud protection mechanisms put in place by them to protect user interests.

[5] https://www.tatatrusts.org/our-work/digital-transformation/digital-literacy/internet-saathi
[6] https://en.wikipedia.org/wiki/Digital_Unlocked

Q.17. Whether there is a need to develop a regulatory framework for the responsible development and use of Metaverse?

Yes, there is definitely a need to develop a regulatory framework for the responsible development of the metaverse. As any regulatory framework has to be designed with the twin objective of identifying potential risks/ mischiefs and with incentivizing positive outcomes for the public at large, we first deal with some risks that unregulated development and misuse of the metaverse may pose. Subsequently, in Part -II of our response, we will list the various systems to be adopted and explored to mitigate these risks and those indicated in the question under reply.

As the metaverse is a chimeric beast, we have researched risks identified by various stakeholders, industry and academics to arrive at a comprehensive list of risks that users of the metaverse may face as this field grows and evolves. We do caveat our response with the fact that as the suite of metaverse technologies evolve, novel risks may emerge which we cannot foresee today.

A comprehensive summary of the risks that are to be expected from the metaverse can be visualized as the following framework[7]:

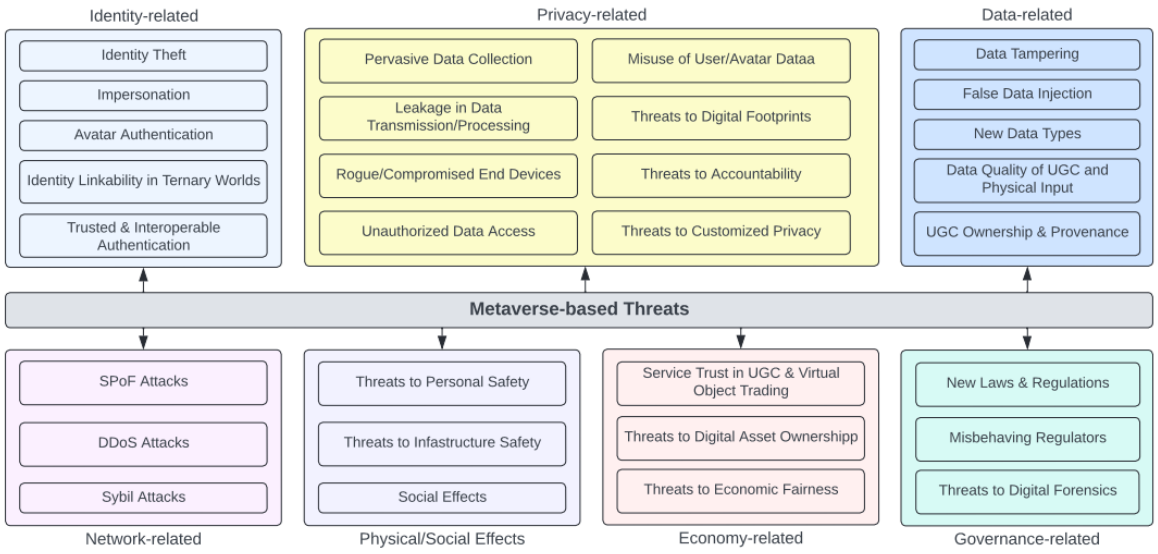

Fig. 3: A brief summary of major Metaverse-based threats [6].

[7] https://eprints.qut.edu.au/236699/1/118427338.pdf

We have summaries these risks, and mischiefs, that any regulatory framework would have to be designed to manage and mitigate:

1. **Identity-Related Risks**:- Identity-related risks encompass threats such as identity theft, impersonation, avatar authentication issues, identity linkability, challenges in achieving trusted and interoperable authentication, third-person perspective and social engineering attacks. These risks undermine users' control over their digital identities within the metaverse. These identity-based risks can occur in the following ways:-

    a. In the metaverse, **identity theft**[8] involves the unauthorised use of personal information and likeness to create a digital avatar, with no current safeguards against this practice. This raises concerns as these digital impersonations can be used for deceptive purposes, especially when combined with AI technologies like deep fakes, which can convincingly mimic a person's appearance and behaviour.

    b. **Digital impersonation** involves using someone's name, image, or other identifiers for dishonest or deceitful purposes. In the metaverse, this can mean things like stealing someone's online identity or taking control of their accounts.

    c. **Identity Linkability**[9] in ternary worlds encompasses the physical, digital, and human realms, all of which are interconnected within the metaverse. This integration potentially enables malicious individuals to monitor users and ascertain their real-world locations. Additionally, hackers could potentially trace users by exploiting compromised headsets and other wearable devices.

    d. A further concern in this category is the **Third Person Perspective**[10], which permits users to move the camera independently of their avatar, potentially enabling covert observation and spying on other avatars without their knowledge, thereby intruding on their privacy. Additionally, there is the risk of compromising biometric data, including brain signals, eye movements, and

[8] https://www.lexology.com/library/detail.aspx?g=0dacec5f-08cd-44e7-8137-6fb161bf92de#:~:text=Identity%20theft%20in%20the%20metaverse,a%20person%27s%20identity%20and%20likeness.
[9] https://identitymanagementinstitute.org/metaverse-security-and-privacy-threats/#:~:text=Identity%20linkability%20in%20Ternary%20Worlds&text=All%20three%20are%20integrated%20into,headsets%20and%20other%20wearable%20devices.
[10] https://www.academia.edu/62933358/Privacy_Regulation_in_the_Metaverse

body movements. This data can be exploited to create fake avatars or reveal personal information about users.

e. **Social engineering attacks**[11] like doxing, stalking, bullying, and fraud may also exploit users' behaviour and communication patterns.

2. **Data-Related Risks** pertain to issues like data tampering, false data injection, the emergence of new data types, and concerns about the quality of user-generated content and physical input data. These risks undermine the integrity and reliability of the data collected and processed within the metaverse. These data-related risks can play out in the following ways:-

   a. A **data tampering attack** involves the alteration of data during its transmission across different platforms within the metaverse. The integrity safeguards are responsible for detecting any changes made to this data, be it in the physical world, virtual environments, or avatars. Attackers may manipulate, change, delete, or substitute this data to disrupt physical objects, users, and their digital representations. These malicious actors can avoid detection by falsifying log records or message-digest outcomes.

   b. A **false data injection attack** pertains to the introduction of counterfeit information, such as messages and commands, with the aim of deceiving metaverse systems. For instance, attackers may manipulate artificial intelligence models by incorporating adversarial training data during the training process.

   c. The metaverse introduces a variety of **novel data types,** each with its distinct implications. For instance, User Attention Points, derived from eye-tracking technology, offer valuable insights for both businesses and researchers, potentially emerging as a key performance metric in the metaverse. Spatial data, which accounts for the three-dimensional virtual environment, becomes pivotal in refining user experiences. Facial expression tracking provides a deeper understanding of user emotions, benefiting brands by augmenting engagement, marketing effectiveness, and fostering innovation. Additionally, economic behavior patterns, encompassing aspects like savings and

11 https://pdfs.semanticscholar.org/5f38/8319ca6640bb10265fa73dd69bbce9d7bdf2.pdf?_gl=1*1k47wa2*_ga*MTA3Mjk1OTU4OS4xNjk1NTQ4NjEw*_ga_H7P4ZT52H5*MTY5NzEyNzQ1My4zMC4xLjE2OTcxMjc3MjEuMTguMC4w

entrepreneurial endeavors, yield valuable marketing data while raising considerable data privacy concerns, possibly necessitating future regulatory measures. While these data types hold the promise of transforming user experiences and marketing strategies, their ethical and privacy dimensions must not be disregarded.

3. **Privacy-Related Risks**:- Privacy-related risks involve challenges such as pervasive data collection, data leakage during transmission or processing, threats from rogue or compromised end devices, unauthorised data access, misuse of user/avatar data, threats to digital footprints, accountability issues, and customized privacy threats. These risks impact the confidentiality and anonymity of users' personal and sensitive data in the metaverse. Furthermore, vulnerabilities in VR headsets may allow attackers to access the user's camera, microphone, or sensory data or manipulate their sensory experience within the virtual environment.

4. **Network-Related Risks**:- Network-related risks encompass single point of failure attacks, distributed denial-of-service attacks, Sybil attacks, and threats to personal and infrastructure safety. These risks affect the availability and resilience of the network infrastructure and services in the metaverse, in the following ways.

   Centralized architectures[12] like the cloud-based systems commonly used in creating the metaverse offer convenience and cost-efficiency. However, they are susceptible to **Single Points of Failure (SPoF)**, which can result from physical server damage or **Distributed Denial-of-Service (DDoS) attacks**. Additionally, these architectures can hinder the seamless exchange of tokens or virtual currency across different metaverse domains. DDoS attacks, for instance, can be executed by hackers who leverage IoT botnets comprising numerous IoT devices, overwhelming the centralized server with excessive traffic, leading to service disruptions and network failures. Furthermore, **Sybil Attacks** involve adversaries manipulating multiple stolen identities to gain disproportionately significant influence in metaverse services, particularly those relying on reputation and voting systems, thereby compromising the overall system effectiveness.

5. **Economy-Related Risks**:- Economy-related risks involve threats to digital asset ownership, economic fairness, trust in user-generated content and virtual object

[12] https://identitymanagementinstitute.org/metaverse-security-and-privacy-threats/

trading services, as well as threats to physical and social effects within the metaverse. Additionally, there's a concern about the potential consolidation of monopolies in the metaverse era. Large tech giants, like Facebook (Meta), may design products that integrate various applications into a single system, posing security risks. Such consolidation could also result in an imbalance of power, where a dominant player has significant control over user data and interactions with third parties, which is a risk applicable to any tech giant in the metaverse.

6. **Governance-Related Risks**:- Governance-related risks include challenges related to new laws and regulations, digital forensics threats, regulatory misbehavior, and potential violations of digital human rights. These risks affect the legal and ethical aspects of the metaverse and its users. An additional concern is the integrity and authentication challenges faced in distinguishing between humans, software agents, and bots, along with ensuring the accuracy and consistency of data in the metaverse. These risks can manifest in the following manner:

    a. **Service Trust Issues in Virtual Object Trading:** Inherent fraud risks like repudiation and payment refusals during virtual object transactions can erode trust within the metaverse marketplace. To ensure trust, the metaverse must guarantee the authenticity and reliability of digital objects created through digital twins.

    b. **Threats to Digital Asset Ownership:** The absence of a central authority and complex ownership structures make it challenging to generate, price, trade, and trace the ownership of digital assets in the trading economy. This includes collective and shared ownership.

    c. **Threats to Economic Fairness in the Creator Economy**: To maintain fairness in resource sharing and digital asset trading, well-designed incentives are essential. However, three factors jeopardise this fairness:

        - Strategic users or avatars can manipulate the digital market to exploit supply and demand imbalances for substantial profits.
        - Free-riding users or avatars gain revenue and use metaverse services without contributing, risking the sustainability of the creator economy.
        - Collusive users or avatars may collaborate or a service provider to manipulate the market and reap profits.

7. **Mental Health Risks**: Some of the mental health issues[13] that may arise from using Metaverse are:

    a. Addiction: Users may become addicted to the virtual world and neglect their real-life responsibilities and relationships. They may also experience withdrawal symptoms when they are offline.
    b. Anti-social personality disorders: Users may lose their social skills and empathy due to the lack of physical human interactions. They may also develop aggressive or manipulative behaviours in the virtual world that can affect their real-life relationships.
    c. Depression: Users may feel depressed due to the isolation, loneliness, or dissatisfaction with their real-life situations. They may also compare themselves negatively with other users who have more attractive or successful virtual avatars.
    d. Inferiority or superiority complexes: Users may develop low self-esteem or overconfidence due to unrealistic and distorted representations of themselves and others in the virtual world. They may also feel insecure or arrogant about their real-life identities and achievements.

It may be noted that these risks are not novel to the metaverse, and are creatures of the web2 revolution, but they stand to be greatly amplified by the proliferation of the metaverse.

In conclusion, developing a regulatory framework for the responsible growth of the metaverse is imperative. This framework must balance the identification of potential risks and misuses with the promotion of positive outcomes for the public. The metaverse introduces a multitude of risks in various domains, and it is crucial to address them systematically. These risks encompass identity-related concerns, data-related issues, privacy challenges, network vulnerabilities, economic threats, and governance-related risks. Additionally, the metaverse poses mental health risks, including addiction, anti-social behaviors, depression, and the development of inferiority or superiority complexes. It is important to acknowledge that while these risks are not entirely new, they are greatly amplified in the metaverse, underlining the urgency of proactive regulation and ethical considerations for this emerging digital frontier.

---

13 https://pdfs.semanticscholar.org/5f38/8319ca6640bb10265fa73dd69bbce9d7bdf2.pdf?_gl=1*1k47wa2*_ga*MTA3Mjk1OTU4OS4xNjk1NTQ4NjEw*_ga_H7P4ZT52H5*MTY5NzEyNzQ1My4zMC4xLjE2OTcxMjc3MjEuMTguMC4w

i. How can users control their personal information and identity in the metaverse?

iv. How can data privacy and security be ensured in the metaverse, especially when users may have multiple digital identities and avatars across different platforms and jurisdictions?

The answers to questions (i) and (iv) will have significant overlaps, thus they are being answered together. The core issues that require answering is how users can protect/ control and secure their personal data/ information, which data/ information is directly tied to their identities. This issue becomes especially tricky, as one individual/ person/ user may own and control multiple sub-identities/ avatars.

A multi avatar / identity world aids in data protection and privacy, though such a scenario may make enforcing regulations difficult, if not impossible, in certain scenarios. For this reason, a balanced approach has to be adopted, which ensures maximal identity abstraction/obfuscation on the one hand - when public facing; and complete identity transparency when regulator facing.

In this light we make (and borrow) the following suggestions:

1. **Avatar Traceability in the physical world[14]:** To ensure data security, privacy and identity management in the metaverse, secure authentication framework that addresses the challenges of ensuring the virtual-physical traceability and consistency of avatars, may be required. This could include:

    a. **A secure authentication framework for metaverse**: a framework that can track a malicious avatar to its physical player and verify the consistency of the avatar's virtual and physical identities.

[14] https://arxiv.org/pdf/2209.08893.pdf

b. **Chameleon collision signature algorithm**: a potentially efficient algorithm that can sign multiple messages with one key pair and generate collisions to form signatures, which ensures the verifiability of the avatar's virtual identity.

c. **Avatar's identity model**: a model that combines the chameleon signature and the biometrics to link the avatar's virtual identity and physical identity, which prevents disguise and impersonation attacks.

d. **Decentralized avatar authentication protocol**: a set of two protocols that can achieve dynamic and mutual authentication between avatars without involving a trusted third party and also establish a session key for secure communication.

2. **Soul bound tokens**[15]: Soulbound Tokens ("**SBTs"**) emerge as a significant innovation to secure avatars and uphold privacy in the metaverse. Their non-transferability is central to establishing unique digital identities, thereby deterring the malpractices associated with transferable assets, like the Pay to Win mechanism. Platforms like Arcomia and Astral Pioneers illustrate the practical application of SBTs in fostering a blend of identifiable and anonymous interactions in the metaverse, thereby paving the way for a more secure and privacy-compliant virtual environment.

   These SBTs can be issued by regulated entities and can form the base layer for online anonymous digital interactions. On the internet, multiple avatars can be 'minted' with the SBT as the parent token. This will allow anonymity as a default right, with the anonymity only being pierced in case of cyber crimes or other violations.

   Using SBTs it will possible to abstract an identity, so that those who only need to ensure two types of trusted information - for example - age and citizenship, will be able to only read this limited information from a SBT (similar to how we allow cookies on websites), and not other information -like name, gender, residential address, blood group, photograph, etc.

3. **Registration of avatars like companies**[16] The paper, "*Avatars in the metaverse: potential legal issues and remedies*", argues that all avatars in a

[15] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4105763
[16] https://link.springer.com/article/10.1365/s43439-022-00056-9

metaverse should be subject to registration, similar to how a company is incorporated. Just like companies, avatars are non-human, and both can exist to increase economic investments in the marketplace. There is a case to be made that whatever rights have been extended to companies should also extend to avatars to increase productivity, and that an avatar may belong to more than one individual- similar to how an instagram account may be managed by more than one individual though the account is credited to one individual. Additionally, the concept of causation and foreseeability would have to be expanded under negligence law[17], for instance, to cover harm caused by avatars or infrastructures in the metaverse.

4. **Informational privacy**, where the user is in a position to determine for one self when, how and to what extent information about one self is communicated with others, therefore allowing individuals to define social contexts in which they present different aspects of themselves. This may be achieved to specific protocols and SBTs.

5. **User centric interventions and behaviour chance** would also be necessary to ensure the regulatory objectives are met, and this may include:

    a. Using **multifactor authentication** and **identity-verification protocols**, especially for higher-risk transactions or interactions, such as money movement or meeting celebrities. This can help prevent digital impersonation and fraud.

    b. Choosing platforms and ecosystem partners that have **ethical standards, transparency, and accountability** for data collection and use. This can help protect data privacy and prevent data misuse.

    c. Leveraging innovations and integrations with **passwordless authentication protocols,** such as FIDO credentials[18] or verifiable credentials (VCs). This can help reduce the risk of phishing and social-engineering attacks.

    d. Training and awareness surrounding how to spot potentially fraudulent, non-validated identities and assets in different metaverses. This can help avoid

[17] https://www.formativelaw.ca/2020/08/part-2-potential-tort-liability-arising-from-virtual-reality-roblox-and-beyond/
[18] https://media.fidoalliance.org/wp-content/uploads/2022/03/How-FIDO-Addresses-a-Full-Range-of-Use-Cases-March24.pdf

losing access to exclusive assets and crypto wallets due to account takeover or credential replay attacks.

6. **Security of virtual reality authentication methods in metaverse[19]:** Given how important authentication would be on the metaverse, we analysis the various authentication methods employed in virtual reality environments, including information-based, biometric, and multi-model methods, highlights the security implications of these methods. These include:

   a. **Information-Based authentication,** which is predominantly utilized, requires a user to provide a PIN or alphanumeric password to access the Metaverse universe. Through meticulous studies and a two-stage testing phase focusing on both usability and safety, various authentication mechanisms like 3D patterns, pattern locks, and PIN systems have been scrutinized. Notably, the 3D pattern emerged as the most secure yet less user-friendly as compared to the PIN system. The evaluation, which encompassed measuring verification time, error rate, and vulnerability to shoulder surfing by monitoring hand movements during password entry, illuminated the pressing need for enhanced interface designs to mend the observed inverse relationship between usability and reliability.

   b. **Biometric authentication**, on the other hand, hinges on employing unique biometric data for verification, with Electroencephalography (EEG), body movements, and Electrooculography (EOG) readings being frequently used. However, a significant concern arises from the conversion of users' biometric data into data, as this process can potentially introduce vulnerabilities, thus casting a shadow on the impeccable reliability of biometric data.

      Biometric authentication may also include innovations like 'Blinkey'[20] for securing VR devices. This method utilizes eye-tracking for user authentication, where authentication is achieved by blinking eyes according to a known rhythm, exhibiting an average error rate of 4%. Such unique authentication methods could significantly mitigate common cyber threats like zero-effort, statistical, shoulder-surfing, and credential-aware attacks, thus protecting users from unauthorized access and potential harassment.

[19] https://arxiv.org/abs/2209.06447v1
[20] https://journal-home.s3.ap-northeast-2.amazonaws.com/site/2022f/abs/LVEIW-0191.pdf

c. **Multi-model authentication** elevates security measures by necessitating the amalgamation of two or more authentication techniques for user login. For instance, the RubikBiom[21] model encapsulates this method by correlating biometric behaviors captured during authentication with a password input on a rubik's cube, enhancing security robustness. A variant of multi-model authentication, Gaze-Based Authentication[22], leverages human eye movements for verification. This method, while necessitating specialized devices for certain actions like fingerprint scanning, showcases a low error rate and an average input time of 5.94 seconds, making it a promising avenue for secure yet efficient user authentication in virtual reality settings.

In synthesizing these suggestions, one discerns a consistent theme: the intersection of innovation and regulation in fostering a secure and transparent digital ecosystem. Strategies such as Avatar Traceability and Soulbound Tokens (SBTs) promise a dual approach—offering users the freedom to abstract their identities for public consumption while also creating mechanisms for regulatory oversight. Coupled with robust authentication frameworks that embrace both traditional PIN systems and avant-garde biometrics, these suggestions lay the groundwork for an evolved digital jurisprudence.

Furthermore, the proposal for avatar registration akin to corporate entities showcases the necessity to adapt existing legal frameworks to encapsulate the unique challenges posed by metaversal existence. Such a mechanism could extend corporate rights and responsibilities to avatars, thereby bringing them within the purview of existing laws and perhaps necessitating the creation of new ones. This regulatory net tightened but flexible, seeks not just to govern but to empower, enabling users to define and defend their manifold identities.

In conclusion, the bedrock for secure interaction in the metaverse will be laid by a holistic approach that marries technological innovation with regulatory agility. Secure, transparent frameworks for avatar traceability, the inventive use of SBTs, and pragmatic legal adaptations offer a balanced approach to identity management. When executed in concert, these strategies promise not just a reactive set of regulations, but a proactive ecosystem designed for the safe, efficient, and ethical use of the metaverse. This

[21] https://dl.acm.org/doi/abs/10.1145/3334480.3382799
[22] K. LaRubbio, J. Wright, B. David-John, A. Enqvist and E. Jain, "Who do you look like? - Gaze-based authentication for workers in VR," 2022 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW), Christchurch, New Zealand, 2022, pp. 744-745, doi: 10.1109/VRW55335.2022.00223.

ecosystem would accord users the privacy they desire and regulators the oversight they require, striking a judicious balance in the labyrinthine world of virtual identities.

ii. How can users protect themselves from cyberattacks, harassment and manipulation in the metaverse?

The suggestions made hereinabove would go a long way in protecting users from cyber attacks, harassment and manipulation ("cybercrimes") in the metaverse, in additional to general awareness through public messaging, educational out reach to the most vulnerable. In addition to the above, the following may also be considered:

1. An effective user facing tool that can be deployed as a regulatory-technology interface might be Cyber Threat Intelligence (CTI)[23] sharing, which can serve as a protective measure against these challenges. The introduction of user-centric CTI sharing will enhance security, benefiting all stakeholders, from users to telecom providers.

2. The development of **ethical standards** and **best practices** for data collection, processing, and sharing in the metaverse, as well as ensuring **transparency and accountability** of data practices by metaverse-based organizations and users, would be pivotal.

3. Fostering **public awareness** and **education** on the potential benefits and risks of the metaverse, as well as empowering users to control and protect their personal data and digital assets.

4. Leveraging **blockchain technology and smart contracts** to enable decentralised, secure, and trustworthy data management, digital asset ownership, and economic transactions in the metaverse.

5. Establishing **legal and regulatory frameworks** that allow affected users to report cybercrimes, similar to UCC model currently in use.

6. To protect user privacy in the metaverse through **terms of service**, it's crucial to provide clear information about data collection, use, and sharing, obtain explicit

[23] https://www.semanticscholar.org/paper/The-Role-of-Cyber-Threat-Intelligence-Sharing-in-Dunnett-Pal/04646b7947c6eafb810de42e6832f79b53fce854

user consent, implement robust security measures, allow data access and deletion, comply with relevant regulations, and educate users about their privacy rights. Regularly update your terms of service to reflect changing laws and technologies in the metaverse while ensuring transparency and user control over their data. Consulting with legal experts is essential for tailoring your terms to your specific metaverse platform and jurisdiction.

7. **Deepfake Detection:** Deepfakes[24] pose a substantial threat in the metaverse, where they could be employed to manipulate or harass users. A lip-based speaker authentication system to combat deepfake attacks, particularly those manipulating visual speaker authentication systems may be a good starting point. Ultimately, a sophisticated deepfake detection systems would be necessary to minimize users' risk of manipulation and maintaining the integrity of their interactions within the metaverse. The core issue with all forms of AI based information will be provenance detection, discussed in detail below.

iii. How can users trust the content and services they access in the metaverse?

In additional to the solutions proposed in answer to the other questions, the following solutions may be considered.

1. **Sharable NFTs:** Shareable Non-Fungible Tokens (sNFTs) – a creature of latest amendments to the Ethereum protocol (with other blockchain protocols swiftly following suit) may be an instrument for fostering trust, traceability, and collaboration within the metaverse. These sNFTs can solve the provenance problem by ensuring all shared content is traceable on the blockchain. This can be an elegant and simple solution to a lot of the problems of fraud feared on most digital platforms, ecosystems including on the metaverse.

   Importantly, sNFTs act as digital markers for non-scarce resources like multi media content, contributions and achievements, enabling mutual recognition and appreciation among participants. For instance, a shareable NFT earned by one individual can be extended to another as a testament to collective effort. Secondly, these NFTs facilitate the creation of a verifiable graph detailing the lineage and

[24] https://journal-home.s3.ap-northeast-2.amazonaws.com/site/2022f/abs/LVEIW-0191.pdf

impact of shared digital assets. This graph not only authenticates the origin but also evaluates the quality of content and services, thereby forming a traceable tree-like structure of sharing activities.

Shareable NFTs capture positive externalities, incentivizing a culture of collaboration. The act of sharing these tokens amplifies social capital by forging new relationships and enhancing existing ones, thereby elevating the overall trust and cooperative ethos within the metaverse.

2. **AI Screening of Content:** Implementing Artificial Intelligence (AI) for screening content can be a formidable line of defense against misinformation, inappropriate content, or malicious activities. AI algorithms can analyze vast amounts of data to detect anomalies, verify facts, or filter out unwanted content, thus ensuring a safer and more reliable user experience. (See our content moderation answer below)

3. **Privacy and Authentication by Design:** Integrating privacy and authentication mechanisms from the ground up in the design of metaverse platforms can significantly enhance trust. By ensuring that user data is protected and that individuals are who they claim to be, users can interact with content and services with a higher degree of confidence.

4. **Additional Measures:** Educating users on how to navigate the metaverse safely, verifying the identities of content and service providers, and establishing a robust legal framework to address disputes and malpractices are also crucial steps towards building trust.

Q.18. Whether there is a need to establish experimental campuses where startups, innovators, and researchers can collaborate and develop or demonstrate technological capabilities, innovative use cases, and operational models for Metaverse? How can the present CoEs be strengthened for this purpose? Justify your response with rationale and suitable best practices, if any.

Part I – The Need for Experimental Campuses

There is a dire need for experimental campuses ("**ECs**") and regulatory sandboxes, all of which enable and empower startups, innovators and researchers to collaborate in a secured environment, explore innovative use-cases as well as operational models.

In an era of emerging technologies where the very nature of technology being studied, used and regulated changes at hypersonic speeds, a static model of innovation and regulation is no longer viable. This is why innovation and regulation must go hand in hand. To achieve this, an appropriate mechanism is needed to ensuring the right incentives are provided, and received by the intended recipients. This mechanism should be channeled through experimental campuses working in collaboration with various regulators.

When looked at from an international lens, we find that many countries have started experimental campuses and are actively engaged in studying, developing and regulating the metaverse.

For example, experimental campuses are already being established in some universities in the United States of America, such as Morehouse College, which has established a digital twin campus to teach classes across a range of subjects including chemistry, biology, business, and journalism[25], with many schools and colleges actively looking to leverage the metaverse for educational purposes[26].

Countries such as Singapore, Indonesia, and South Korea are already starting to experiment with the metaverse and will likely develop their regulatory approach in collaboration with industry[27]. The European Union has put in place a regulatory framework across its member countries, while in the United States of America (USA),

[25] https://about.fb.com/news/2023/09/metaverse-technologies-education-opportunities/
[26] https://axonpark.com/7-reasons-why-your-school-should-be-prepping-for-the-metaverse/
[27]https://www.gsma.com/publicpolicy/the-year-ahead-in-digital-policy-regulating-the-metaverse

individual states are legislating piecemeal, and there is limited federal law.[28] [29] The US Congress is more likely to take a 'wait and see' approach to metaverse regulation.[30] The metaverse provides schools with an opportunity to utilize spatial computing and artificial intelligence to enhance the student experience and improve learning outcomes. [31]

In this context, we list below the various benefits that experimental campuses can have for innovators, creators/builders, emerging or establishing businesses/industries, academia and Government of India:-

1. **Innovation and Research Collaboration:** Collaborative spaces encourage cross-disciplinary interactions, enabling innovators from different domains to come together and explore new ideas. This environment can lead to innovative solutions and use cases that might not emerge in more traditional settings. The example of Stanford University and its outsized impact on Silicon Valley is the case in point[32]. Activities within these campuses can stimulate economic growth by supporting startups and creating jobs, as was done with Silicon Valley. However, given the decentralized nature of the current web3/ metaverse revolution, India should aim for multiple technology hubs spread out over the entire country to ensure equitable growth and maximal talent utilization.

2. **Rapid Prototyping and Testing:** These campuses can serve as testing grounds for new technologies and applications. Startups and researchers can build prototypes and test them in real-world scenarios, allowing for rapid iteration and refinement. The Massachusetts Institute of Technology (MIT) in the United States has an Innovation Initiative that offers resources and support for rapid prototyping and testing of emerging technologies, facilitating the creation of groundbreaking innovations, and is a good example of academia collaborating with industry in a safe haven[33].

3. **Regulatory Sandboxes for Policy Development:** Regulatory sandboxes within campuses create controlled environments for startups to test their ideas, allowing policymakers to shape regulations while fostering innovation. Some examples of regulatory sandboxes for emerging technologies in existence around the world including in India are:

[28] https://www2.deloitte.com/us/en/insights/industry/technology/emerging-regulations-in-the-metaverse.html
[29] https://gammalaw.com/eu-to-launch-global-metaverse-regulation-in-2023-will-the-us-follow-suit/
[30] https://www.gsma.com/publicpolicy/the-year-ahead-in-digital-policy-regulating-the-metaverse
[31] https://axonpark.com/7-reasons-why-your-school-should-be-prepping-for-the-metaverse/
[32] https://techcrunch.com/2015/09/04/what-will-stanford-be-without-silicon-valley/#.svc0u6:dNI0
[33] https://innovation.mit.edu/about/

a) Singapore: The Monetary Authority of Singapore (MAS) has set up a regulatory sandbox for fintech companies, which includes blockchain and distributed ledger technology (DLT) companies. The sandbox allows companies to test their products and services in a controlled environment, with the aim of promoting innovation in the financial sector[34].

b) United Kingdom: The Financial Conduct Authority (FCA) has set up a regulatory sandbox for fintech companies, which includes blockchain and DLT companies. The sandbox allows companies to test their products and services in a controlled environment, with the aim of promoting innovation in the financial sector.[35]

c) India: The Reserve Bank of India (RBI) has set up a regulatory sandbox for fintech companies, which includes blockchain and DLT companies. The sandbox allows companies to test their products and services in a controlled environment, with the aim of promoting innovation in the financial sector.[36]

4. **Talent and Skill Development:** Experimental campuses provide educational programs to nurture talent in emerging technologies. Since India has a young demographic who are still in colleges, schools and universities, and they are the future user base and workforce, it serves the public good well[37] to involve the students at the ground floor, increase the scope for digital employment[38] and buck the trend of youth disengagement[39] This is a healthy trend that should be guided and protected in the safe confines of experimental campuses.

Part II: Next Steps

To realize the benefits of experimental campuses it may not be necessary to create a new framework from scratch, but rather to leverage/ strengthen the existing experimental campuses including CoEs. We propose the following steps that can be implemented by ***a)*** government agencies, ***b)*** Educational Institutions, ***c)*** Industry bodies, ***d)*** Community institutions, to unlock the benefits mentioned in Part I of our answer above by establishing a network of collaborative CoEs/ ECs :-

1) Government Agencies:

[34] https://www.mas.gov.sg/development/fintech/regulatory-sandbox
[35] https://www.fca.org.uk/firms/innovation/regulatory-sandbox
[36] https://www.rbi.org.in/Scripts/BS_ViewBulletin.aspx?Id=19899
[37] https://www.imf.org/en/Blogs/Articles/2019/01/22/blog-unlimited-opportunities-creating-more-jobs-for-young-people
[38] https://www.ilo.org/wcmsp5/groups/public/---dgreports/---dcomm/---publ/documents/publication/wcms_853321.pdf
[39] https://blogs.worldbank.org/education/youth-economic-disengagement-harsh-global-reality-remember-world-youth-skills-day

a) **SEZs:** Special Economic Zones (SEZs) in India can align their focus with emerging technologies and innovation. By promoting tech-oriented businesses and facilitating easy setup, SEZs can become centers for technological innovation.

   Example - In **Singapore**, the government has designated the Punggol Digital District[40] as an SEZ, focused on nurturing emerging technologies including the Metaverse, to create a conducive environment for Metaverse-related innovation.

   In fact, an SEZ need not be terrestrial anymore—Japan has pioneered the Japan Metaverse Economic Zone within the metaverse itself with leading industry players[41]. A metaverse economic zone is a cross-border SEZ based in the metaverse. The purpose of a metaverse economic zone is to develop a digital space where businesses can operate across borders, through legally-compliant and interactive environments, and cater to multinational corporations, decentralized autonomous organizations, and individuals. This can help a country or organization grow in the developing digital economy. A metaverse economic zone will also support the establishment of a framework for corporations to develop Web3 marketing, work reform, and consumer experience initiatives.

b) **Tax incentives**: The Indian government can introduce targeted tax incentives and amendments to the Income Tax Act 1961 and Central Goods and Services Tax 2017 to encourage research and development activities within existing experimental campuses, as has been done with the GIFT City[42]. Depreciation for Metaverse infrastructure, R&D tax credits, GST exemptions or reductions, custom duty waivers, capital gains tax benefits, and investment promotion zones may also be considered. These incentives aim to reduce the tax burden on Metaverse businesses, spur innovation, and attract domestic and foreign investments, ultimately fostering the growth of the Metaverse ecosystem in India.

c) **Mission-based Grants and Funding:** Government ministries and departments can allocate mission-specific grants and funding to Metaverse/Web3-focused CoEs. This involves identifying key technology domains within the Metaverse, such as virtual reality, augmented reality, or blockchain integration, and providing targeted financial support to CoEs dedicated to advancing these domains. These funds are designed to drive innovation, research, and development in Metaverse-related

[40] https://www.channelnewsasia.com/singapore/new-500-million-technology-innovation-centre-punggol-digital-district-completed-end-2026-3428461
[41] https://www.fujitsu.com/global/about/resources/news/press-releases/2023/0227-02.html
[42] https://www.investindia.gov.in/team-india-blogs/unlocking-opportunities-exploring-potential-gift-city-financial-hub#:~:text=To%20attract%20businesses%20to%20GIFT%20City%2C%20the%20Government,of%20company%20setup%20as%20a%20unit%20in%20IFSC.

technologies, helping India establish a leadership position in the Metaverse ecosystem by focusing on specific missions and strategic technological advancements.

An example of this is the **Finnish government**, through organizations like Business Finland[43], provides mission-based grants to Metaverse startups working on specific objectives, such as improving virtual healthcare delivery or enhancing virtual education.

d) **Regulatory Technologies**: Regulatory bodies can collaborate with Metaverse-focused CoEs to develop and implement regulatory technologies, often referred to as RegTech. These technologies are designed to streamline regulatory processes and compliance within the rapidly evolving Metaverse landscape. By leveraging RegTech, regulatory bodies can keep pace with the dynamic nature of Metaverse technologies, ensuring that regulations remain up to date, efficient, and effective. This collaboration not only enhances regulatory oversight but also fosters an environment where Metaverse innovation can thrive, as businesses can navigate the regulatory landscape more efficiently and with greater clarity.

   An example of this is **Australian Securities and Investments Commission (ASIC)** collaborates with industry stakeholders to develop RegTech solutions that streamline regulatory processes within the Metaverse sector, ensuring compliance and security[44].

e) **Ministry-based Sandboxes**: Ministries in India, spanning domains like healthcare, education, or transportation, can establish specialized sandboxes within ECs/ CoEs that focus on the Metaverse and it's base technologies being blockchain, AR/VR/MR and AI/ML. These sandboxes serve as controlled environments where the ministries can explore how Metaverse technologies align with their specific objectives and missions.

   For example, the Ministry of Education can utilize a Metaverse sandbox to test immersive educational experiences or scale virtual classrooms[45]. The Ministry of Healthcare can explore Metaverse applications for telemedicine and patient care. Similarly, the Ministry of Transportation can assess the integration of Metaverse technologies for urban planning, smart cities, and traffic management.

   These ministry-based Metaverse sandboxes allow government agencies to evaluate the practicality and benefits of Metaverse solutions within their respective

[43] https://www.businessfinland.fi/en/for-finnish-customers/services/funding
[44] https://asic.gov.au/for-business/innovation-hub/asic-and-regtech/
[45] https://mu.ac.in/archives/courses/virtual-classrooms

domains, ensuring that technology advancements are harnessed to meet their objectives and drive innovation in areas critical to the nation's development. A dedicated push for increasing digital penetration and fluency, unprecedented access especially in Tier 2-3 cities, peri urban, rural areas, if done correctly, can foster inclusion and innovation.

2) Educational Institutions:

a) **Provide Physical Infrastructure**: Established universities and educational institutions can contribute to the growth of the Metaverse by offering physical infrastructure. This includes dedicated lab spaces with access to advanced Metaverse related hardware, know-how, and technologies, access to state-of-the-art tech facilities, and student resources. Such support fosters innovation, research, and development in Metaverse-related projects, making educational institutions key contributors to and accelerators of Metaverse COEs.

   An example of this would be the University of California, Berkeley, provides physical infrastructure for its students to develop Metaverse technologies in its XR (Extended Reality) Lab, offering state-of-the-art facilities for research and development.

b) **Incubator Facilities**: Educational institutions play a pivotal role in nurturing Metaverse innovation by expanding their incubator facilities. These expanded incubators offer dedicated spaces, mentorship programs, networking opportunities (matchmaking programs, or access to investors, funds including PE/VC ecosystem), and access to student talent for Metaverse startups. This comprehensive support fosters development, collaboration, and knowledge sharing within the Metaverse sector.

   Example - Stanford University operates an incubator dedicated to Metaverse startups, offering resources, mentorship, and networking opportunities within its campus.

c) **Teacher-Student Collaboration**: Encouraging collaboration between faculty and students on projects within educational institutions can lead to innovation and academic research resulting in an increased number of peer reviewed publications, laying the groundwork for future innovation.

d) **Academic Research:** Educational institutions can focus their academic research efforts on emerging technologies that align with the mission of existing CoEs by establishing dedicated departments and curriculum.

e) **Dedicated Coursework:** Educational institutions can boost the Metaverse ecosystem by developing specialized coursework that equips students with essential skills and knowledge in Metaverse technologies. These courses prepare students for careers in Metaverse-related fields and align with industry demands, ensuring a workforce ready to drive innovation and development in the Metaverse sector.

f) **Collaborative Relationships:** Educational institutions can establish collaborative and competitive relationships with other CoEs to share knowledge and resources, benefiting from each other's strengths.

g) **Access to Regulators:** Institutions can create avenues for their students to access regulators and policymakers, facilitating an understanding of the regulatory landscape.

Students from a Metaverse-focused program can participate in a dialogue with the Reserve Bank of India (RBI), SEBI, state and central law makers, Ministry departments, law and order enforcement agencies, amongst others to explore the impact of Blockchain/ VDAs/Web3; AI/ML and AR/VR/MR on the Metaverse and structure their products, services and corporate entities accordingly to ensure high compliance.

Students can actively participate in discussions and workshops with regulatory authorities. For instance, students may engage with the Telecom Regulatory Authority of India (TRAI) to discuss the implications of Metaverse on communication technologies or with the Ministry of Information and Broadcasting to understand content regulations within virtual worlds. By creating avenues for students to access regulators and policymakers, educational institutions empower the future workforce with valuable regulatory knowledge in the Metaverse domain, promoting responsible and compliant Metaverse development and operation.

3) Industry Bodies:

a) **Establish Standards**: Industry associations like the Bharat Web3 Association, can be called up to lead and generate consensus on establishing standards and recommendations for ethical and responsible use of the Metaverse, addressing issues such as digital citizenship, content moderation, and user safety within existing CoEs/ ECs or those other industry bodies newly created for this purpose.

b) **Grants and Funding:** Industry associations, such as NASSCOM & FICCI can collaborate to fund startups, provide mentorship, and interface with regulators and policymakers to foster a conducive environment for innovation.

c) **Collaborative Relationships:** Industry bodies can establish collaborative relationships with other CoEs and tech-focused organizations to promote knowledge sharing and resource pooling. For example NASSCOM's Gaming Forum, which is a specialized group within NASSCOM can collaborate with CoEs to set industry standards for game development within the Metaverse, covering aspects like game mechanics, virtual economies, and cross-platform compatibility. Internet and Mobile Association of India ("**IAMAI**") can also collaborate and contribute to the creation of standards for Metaverse-related digital marketing and advertising best practices, ensuring that businesses engage with consumers in ethical and effective ways within virtual environments.

4) **Community Institutions:**

1) **CoEs/ECs run by Societies**: Non-profit societies and community organizations can run Centers of Excellence and Experimental Campuses, focusing on specific societal, environmental and/or other local issues. Collaborative relationships with other CoEs can expand their reach and impact.

   For example the Metaverse Society in Canada runs a community-based Center of Excellence that focuses on using Metaverse technology for environmental education, collaborating with other organizations in the area to address local ecological challenges.

2) **Collaborative Relationships:** Community institutions can build relationships with other CoEs to leverage resources, share best practices, and collaborate on innovative projects aimed at addressing local challenges. A non-profit society in a rural area can set up an Experimental Campus focusing on agricultural education through the Metaverse. They can do so by partnering with a larger Metaverse CoE in an urban area to gain access to advanced technology infrastructure and expertise; and jointly develop virtual farming simulations to train local farmers on modern agricultural practices, increasing crop yields and improving the local economy.

Q.19. How can India play a leading role in metaverse standardization work being done by ITU? What mechanism should be evolved in India for making an effective and significant contribution in Metaverse standardisation? Kindly provide elaborate justifications in support of your response.

This answer outlines practical steps that India can take to play a leading role in the standardization of the metaverse, particularly in collaboration with the International Telecommunication Union ("**ITU"**). The proposal focuses on leveraging India's technological expertise, fostering multi-stakeholder collaboration, and aligning efforts with the Sustainable Development Goals (SDGs).

This consultation paper is testament to the fact that the metaverse represents a new frontier in digital technology, offering unprecedented opportunities for social interaction, economic activity, and technological innovation. As the ITU spearheads efforts to standardize this emerging domain, India has a unique opportunity to contribute meaningfully to this global initiative.

Practical Steps for India's Leadership in Metaverse Standardization

1. Identifying other standardization work being done:

a) **Open Metaverse Interoperability Group** (OMG): The OMG is a community-driven initiative that aims to develop open standards for the Metaverse. The group is focused on developing interoperability standards that will enable different virtual worlds to connect and communicate with each other.

b) **Virtual World Framework (VWF):** The VWF is an open-source platform that provides a framework for building virtual worlds. The platform is designed to be flexible and customizable, allowing developers to create unique virtual worlds that can be connected to other virtual worlds.

c) **XR Access Initiative**: The XR Access Initiative is a global initiative that aims to promote accessibility and inclusivity in the development of virtual and augmented reality technologies. The initiative is focused on developing standards and best

practices that will ensure that virtual worlds are accessible to people with disabilities.

d) Joining the Metaverse Standards Forum[46]: India can become a member of the Forum, which is a venue for cooperation between standards organizations and companies to foster the development of interoperability standards for an open and inclusive metaverse. The Forum is open to any organization and has over 2400 members from various domains and regions.

e) **International Organization for Standardization (ISO)**: The ISO is a global organization that develops standards for a wide range of industries and technologies. While there are currently no ISO standards specifically for the Metaverse, the organization could potentially develop standards in the future.

To align with these global standards and initiatives, India could participate in global discussions and collaborate with other countries and organizations to develop standards and best practices for the Metaverse. Additionally, India could leverage its existing digital public infrastructure, such as India Stack, to support the development of the Metaverse and ensure that it aligns with global standards for interoperability, accessibility, and inclusivity. By aligning with global standards and initiatives, India can ensure that its contributions to the Metaverse are effective and significant.

2. **Formation of a National Metaverse Committee ("NMC"):** India must establish a National Metaverse Committee expressly designed to interface with the United Nations' International Telecommunication Union (ITU) Working Group focusing on metaverse standards. Such an institutional arrangement is imperative for several reasons.

    a) ***First***, it will enable a formal, streamlined mechanism for participating in the international standard-setting process, ensuring that India's technological and regulatory perspectives are adequately represented.
    b) ***Second***, it amplifies India's voice in critical discussions concerning the ethical, legal, and social implications of the metaverse, thereby asserting a leadership role in the international community.

[46] https://metaverse-standards.org/

c) ***Third***, by actively participating in the ITU's standardization efforts, India can ensure that the standards developed are amenable to its own national requirements, including considerations of security, interoperability, and inclusivity. Therefore, the National Metaverse Committee would not merely serve as a liaison but as a catalyst for India's ambition to be a frontrunner in shaping the metaverse's global governance architecture.

3. **Public-Private Partnerships for Research & Development:** The National Metaverse Committee may then be tasked with formulating protocols for Public-Private Partnerships (PPPs) in Research & Development (R&D), in a twofold manner:
   a) *Firstly*, PPPs will act as the engine for technological innovation, leveraging both governmental oversight and private-sector agility to accelerate advancements in crucial areas like interoperability, security, and user experience. It is this innovation that India can bring to the table during international standardization discussions, thereby securing a leadership role.
   b) ***Secondly***, PPPs in R&D would facilitate a symbiotic relationship between policy and technology. Through a well-structured PPP framework, the National Metaverse Committee can ensure that the technologies developed are not only cutting-edge but also aligned with the broader objectives of national and international policy, thereby making India's contributions to the ITU's standard-setting both relevant and impactful.

   Thus, by institutionalizing PPP protocols for metaverse R&D, the National Metaverse Committee will be better poised to assert India's role in shaping the global rules governing the metaverse.

4. **Academic Collaboration and Skill Development:** The imperative for India's National Metaverse Committee to develop rigorous protocols for Academic Collaboration and Skill Development is underscored by the nation's strategic objectives to gain ascendancy in the ITU Working Group on metaverse standards. Establishing a symbiotic relationship between academia and policy serves multiple essential functions:

   a) ***Firstly***, it provides a structured framework for cutting-edge research and the development of novel technologies, thereby elevating India's position in international standard-setting bodies through substantial contributions.

b) ***Secondly***, academic-industry collaboration enables the rapid skilling of a workforce proficient in metaverse technologies (blockchain, AI/ML, AR/MR/VR), creating a reservoir of technical expertise. A highly skilled workforce and robust academic foundation lend substantial credibility to India's contributions and aspirations in global standardization forums.
c) Moreover, India's demographic dividend, manifested in a large user base, can become not just consumers but informed participants in the metaverse, further reinforcing the country's credibility.

Therefore, by prioritizing academic partnerships and skill cultivation, the National Metaverse Committee substantially augments India's capacity and credibility to lead and influence the creation of universal metaverse standards, unlocking a level playing field for India's software and hardware sectors to start building on.

5. **Proactive Leadership:** For India to wield substantial influence in shaping the global metaversal landscape, it is paramount that its National Metaverse Committee adopts a posture of proactive leadership within the ITU Working Group on metaverse standards. Proactive interventions would include:

    a) **Regular engagement** with the ITU and other international bodies is not merely advisable but essential. This entails assigning dedicated representatives well-versed in metaverse technologies and policy implications to ITU focus groups. Such representatives can act as the vanguard of India's metaverse initiatives, consistently bringing to the fore India's contributions, innovations, and perspectives, as also leading pilot projects and partnerships around the world to solve the United Nation's Sustainable Development Goals.

    b) **Periodic submission** of meticulously crafted reports and recommendations to the ITU and other pertinent organizations serves dual functions. *Firstly*, it keeps the international community abreast of India's advancements and positions in metaverse technologies, thereby amplifying India's voice in standard-setting dialogues. *Secondly*, it opens avenues for collaborative ventures and policy harmonization, facilitating a unified approach to metaverse reporting and governance. By proactively leading discussions and championing the creation of universal standards, the National Metaverse Committee establishes India as not just a participant but a pioneer in the international metaverse ecosystem.

6. **Strategic Alignment with Sustainable Development Goals for Leadership in Metaverse Standardization:** For India's National Metaverse Committee to assert authoritative leadership within the ITU Working Group on metaverse standards, a robust alignment with the SDGs is critical. By proactively initiating discussions related to how metaverse technologies and standards intersect with SDGs, India can position itself as a thought leader committed to ethical and sustainable technological advancement.

   This stance elevates the discourse beyond mere technical considerations to encompass the broader societal, economic, and environmental implications of the metaverse. Steering such dialogues within the ITU also establishes a framework for global metaverse standards to be intrinsically linked with universally recognized goals of sustainable development. In doing so, India would not only contribute to the creation of holistic and responsible metaverse standards but also ethical best standards and practices to be followed internationally.

   Therefore, by championing the alignment of metaverse standards with SDGs, India’s National Metaverse Committee can significantly enhance the country's influence and credibility in the international standard-setting arena.

Q.20. (i) What should be the appropriate governance mechanism for the metaverse for balancing innovation, competition, diversity, and public interest? Kindly give your response with reasons along with global best practices. (ii) Whether there is a need for a national level mechanism to coordinate development of Metaverse standards and guidelines? Kindly give your response with reasons along with global best practices.

Navigating the governance landscape of the metaverse presents a significant challenge that necessitates a delicate equilibrium between promoting innovation and safeguarding competition, diversity, and the public interest. This challenge is exacerbated by the diverse and rapidly evolving digital ecosystem within the metaverse. A single, rigid approach is insufficient, making it imperative to adopt a multifaceted, minimally intrusive, and comprehensive approach.

This governance architecture should encompass regulatory and governance elements, coordinated by either an existing or a newly established regulatory body. This regulatory authority would be entrusted with the task of overseeing the far-reaching consequences of emerging technologies, including but not limited to the metaverse, artificial intelligence/machine learning (AI/ML), web3, augmented reality/mixed reality/extended reality (AR/MR/XR), and edge computing.

Having said that, the creating a single regulation or statute to regulate the Metaverse may not be the most effective mechanism. An advisory body, made up of key decision makers of the government (in the internet space) as well as representation from the industry, should be set up to take a more advisory role to existing regulators. This will involve the advisory body taking steps such as: (i) identifying the various use-cases or real world deployments of the Metaverse and Web3 technologies and determine whether such application or activity is one that warrants government regulation; (ii) categorize the said activity in terms of the statutory regulators (e.g. SEBI, MCA, RBI, etc.) that would govern the activity; and (iii) make recommendations to the relevant regulators as well as provide an interface to the industry members to make representations and develop regulations while working alongside the regulator. Industry involvement in the creation of regulations for the Metaverse is crucial as the industry will be the first to identify mischief and misuse of the technology. A coordinated approach between the industry and

government will result in creation of comprehensive regulations as well as providing a predictable regulatory landscape fostering development and adoption of new technologies in unique and novel ways. Thus, in place of a single regulator, an advisory body or panel can recommend the amendments to existing legislation that may be required to adopt to the metaverse innovations. Existing regulators can be empowered to monitor and regulate metaverse activities related to their scope. Similarly, one statute may be hard to begin with for governing every activity within the 'metaverse'. Several changes to many statutes may be required before we have an all encompassing legislation. The following lists the various chapters/ sections of existing legislation that can benefit from amendments incorporating the existence of the metaverse technology. The individual elements of the points below have been dealt with comprehensively in response to other questions, for which reason only a summary has been outlined below:

1. **Special Economic Zones (SEZs)**: SEZs serve as crucibles for innovation, providing a fertile ground for experimentation with emerging technologies and business models under a more lenient regulatory framework (a 'regulatory sandbox'). They attract global talent and investments, fostering a competitive and diverse ecosystem. Illustrations: 'Web3 in the sea' planned for Goa and 'RAK DAO' in the UAE.

2. **Standards and Guidelines for Experimental Campuses**: These campuses create a controlled environment for testing, evaluating, and refining novel metaverse solutions. Clearly defined guidelines ensure structured innovation while upholding safety and ethical standards. (See our answer on experimental campuses).

3. **Standards for Metaverse Products, Platforms, and Services**: Robust standards are essential for promoting a level playing field, interoperability, quality, and safety. They reduce barriers to entry for new players, stimulating competition and diversity. (See our answer to Q. 16 and 17).

4. **Regulation of Digital Assets (Sale, Purchase, and Usage):** The virtual economy is central to the metaverse. Ensuring transparency, fair transactions, fraud prevention, and clear ownership rights are vital for a thriving virtual economy.

5. **National Level Coordination Committee:** A centralized coordination mechanism is vital for a unified approach to regulation and policy across metaverse

domains, ensuring consistency, coherence, and effective inter-agency coordination.

6. **International Cooperation:** Collaboration with other nations is necessary to establish international standards for the metaverse, allowing the virtual world to operate cohesively across borders, as well as staying abreast of international policy development.

7. **Intellectual Property Protection**: Enhanced intellectual property protections are needed to address the unique challenges posed by digital assets and creative works within the metaverse. (See our answer to Q.23)

8. **Sectoral Regulator for Emerging Technologies/Metaverse**: A dedicated regulator can offer specialized oversight, expertise and ensure compliance with established standards and guidelines. It serves as a focal point for dispute resolution and responsible metaverse evolution. These sectoral regulators can be created under the existing regulatory framework, supervising their specific industries/activities as carried out over the metaverse.

9. **Online Dispute Resolution (ODR) Standards**: Given the borderless nature of the metaverse, ODR standards are crucial for timely and fair dispute resolution, fostering trust and justice. This is particularly relevant for consumer disputes.

10. **Sovereign Identity/Avatar Management**: Sovereign identity solutions are crucial for privacy, security, and building trust in virtual interactions.

11. **Amendment to the Data Protection Act, 2023**[47]: Existing legal frameworks must evolve to address metaverse-specific challenges, particularly regarding data protection and privacy. In the context of India's Data Protection Act, 2023, adapting to the metaverse necessitates a multi-faceted approach to data privacy. First, the Act should incorporate provisions for recalibrating informed consent mechanisms to account for virtual personas, including age verification techniques. Second, it should establish stringent guidelines for inter-company data transfers, mirroring the GDPR's restrictions on transferring personal data outside its protective ambit. Third, the Act must evolve to address emerging technological challenges, such as targeted advertising based on biological reactions. Fourth, it should bolster existing measures to counter identity theft and unauthorized data

[47] https://jolt.law.harvard.edu/assets/articlePDFs/v36/Martin-Privacy-in-a-Programmed-Platform.pdf

access, issues the metaverse will likely exacerbate. Lastly, timely guidance and updates from regulatory bodies are imperative to ensure that the Act keeps pace with the rapidly evolving metaverse landscape.

12. **Amendment to the Competition Act 2002**: Proposed amendments should introduce and enforce anti-monopoly and anti-trust regulations to prevent monopolistic practices within the metaverse, nurturing a competitive environment.

13. **Fiscal Incentives for Start-ups and Metaverse Businesses**: Fiscal incentives can stimulate innovation, attract investments, and promote entrepreneurial endeavors within the metaverse, contributing to economic growth and job creation.

14. **Local Manufacturing of Hardware Components**: Establishing local manufacturing hubs for metaverse-related hardware fosters self-sufficiency, economic growth, job creation, and innovation. Close coordination between software developers and hardware manufacturers leads to bespoke chip and architecture design, increasing efficiency and processing power. This is made easier if the two services are in the same local area.

15. **Integration of India's Digital Public Infrastructure with the Metaverse**: Merging India's digital public infrastructure with the metaverse can unlock new avenues for public service delivery, citizen engagement, and government-citizen interaction in a secure, efficient, and inclusive manner. The metaverse is a naturally suited technology for distribution of and access to public services.

16. **Workforce Training and Upskilling**: Investment in micro skill development programs equips the workforce with the necessary skills to thrive in the metaverse, bridging the digital divide and fostering economic mobility.

17. **Guidelines on Physical and Psychological Impact**: Establishing guidelines to study and mitigate the physical and psychological impact of prolonged metaverse interaction is essential for user well-being and a healthy virtual environment.

18. **Rapid Response Mechanisms**: Establishing mechanisms for quick responses to emerging issues, such as cyberbullying, harassment, or the spread of harmful content, is essential to protect user well-being.

19. **Mandating Technical Standards by TRAI**: Comprehensive technical standards can ensure a high-quality user experience across various metaverse platforms.

20. **Adaptation of Privacy, Security, and Child Safety Frameworks**: The metaverse's unique challenges require revisions to existing privacy, security, and child safety frameworks, encompassing data encryption, age verification, and user consent conditions.

21. **Regulatory Timing and Context-Sensitivity by TRAI**: A nuanced approach to regulation timing, particularly in sensitive areas like child safety and medical applications, is vital. Regulations should adapt to the fast evolving layer of social and legal contracts and participant expectations in each metaverse platform.

22. **Digital Literacy Promotion and Advocacy**: Collaborative efforts between TRAI, educational institutions, and civil society organizations to enhance digital literacy and awareness are essential for empowering individuals to navigate the metaverse knowledgeably and safely.

23. **Industry-Led Regulatory Technology Solutions**: Industry involvement in developing regulatory technology solutions can proactively identify and mitigate evolving technological risks, ensuring a resilient and secure metaverse ecosystem. Close cooperation between the industry and the regulator can lead to swift regulation of risks identified in the first instance by industry players.

24. **Ethical Content Rating Systems**: Implementing content rating systems that consider ethical and cultural factors is crucial to protect users from offensive or harmful content.

25. **Open Source Initiatives**: Encouraging the use of open-source software within the metaverse enhances transparency, security, and interoperability. Adoption of open source software allows opportunities for the unorganized section of programmers to find new ways to monetize their work.

26. **User Feedback Mechanism**: A robust user feedback mechanism provides valuable insights into user experiences, grievances, and suggestions, informing policy adjustments and ensuring a user-centric and responsive governance framework.

27. **Flexible Approach to Interoperability**: TRAI should consider interoperability as a nuanced, multi-dimensional spectrum, allowing providers to implement varying levels of openness and differentiated services, applying regulations judiciously where complete interoperability might not be beneficial or feasible.

In conclusion, the envisaged governance structure for the metaverse, encompassing these elements, aims to nurture innovation, competition, diversity, and the public interest. Each facet of this regulatory blueprint contributes to forming a governance framework that is resilient, adaptable and scalable to the dynamic nature of the metaverse and its associated technologies. Through the coordinated application of these regulatory and governance elements, guided by a competent advisory body, the metaverse can thrive as a realm of limitless exploration, interaction, and creation, all within a framework of responsibility, equity, and integrity.

Q.21. Whether there is a need to establish a regulatory framework for content moderation in the metaverse, given the diversity of cultural norms and values, as well as the potential for harmful or illegal content such as hate speech, misinformation, cyberbullying, and child exploitation?

Given the diversity of cultural norms and values, as well as the potential for harmful or illegal content such as hate speech, misinformation, cyberbullying, and child exploitation, there is a need to establish a regulatory framework for content moderation in the Metaverse. Here are some reasons why:

1. **Lack of global consensus**: There is little global consensus on how to regulate human behaviors in social experiences, and the Metaverse is no exception. A regulatory framework can help establish a common set of rules and guidelines that all platforms must follow to ensure user safety and prevent harmful or illegal content.[48]

2. **Cross-border content moderation**: Metaverse platforms face challenges in cross-border content moderation, which can have implications for freedom of expression and non-discrimination. A regulatory framework can help establish clear guidelines for cross-border content moderation and ensure that users are protected across all platforms.[49]

3. **Protecting user privacy**: A regulatory framework can help protect user privacy in the Metaverse by establishing clear guidelines for data collection, storage, and use. This can help prevent the misuse of user data and ensure that users have control over their personal information and identity. The present consultation paper with its focus on user privacy in the metaverse is indicative of this need.

4. **Ensuring platform accountability**: A regulatory framework can help ensure that Metaverse platforms are held accountable for their content moderation

[48] https://www2.deloitte.com/us/en/insights/industry/technology/emerging-regulations-in-the-metaverse.html
[49] https://link.springer.com/article/10.1007/s13347-023-00645-4

practices. This can help prevent platforms from adopting the most restrictive content regulations worldwide, severely limiting user expression.[50]

5. **Establishing best practices:** A regulatory framework can help establish best practices for content moderation in the Metaverse. This can help ensure that all platforms are using the most effective methods for moderating content and that users are protected across all platforms.[51]

In summary, a regulatory framework for content moderation in the Metaverse is necessary to address the diversity of cultural norms and values, as well as the potential for harmful or illegal content such as hate speech, misinformation, cyberbullying, and child exploitation. A regulatory framework can help establish clear guidelines for cross-border content moderation, protect user privacy, ensure platform accountability, and establish best practices for content moderation.

[50] https://techhq.com/2023/06/how-is-content-moderation-of-ugc-regulated/
[51] https://www2.deloitte.com/us/en/insights/industry/technology/emerging-regulations-in-the-metaverse.html

Q.22. If answer to Q.21 is yes, please elaborate on the following:

i. What are the current policies and practices for content moderation on Metaverse platforms?

The policies and practices for content moderation on Metaverse platforms are still evolving, and there is little global consensus on how to regulate human behaviors in social experiences.[52]

However, some regulations have been put in place in certain jurisdictions. For example, California's AB 587 requires social networks to post their content moderation policies and provide a description of their processes for flagging and reporting problematic content like hate speech, racism, extremism, dis- and misinformation, harassment, and political interference

Metaverse and proto-metaverse platforms require their users and content moderation to abide by local laws, but local laws may be in conflict. As metaverse platforms become more popular, human moderation will not be feasible at the scale required, and new processes will have to be developed to ensure that content is appropriate. Ultimately, content moderation should not infringe upon the constitutional right of freedom of expression. [53]

Further, content moderation is more difficult for platforms in the metaverse than on social media because the content produced by the interaction between users is not text that will exist for long periods, but a voice chat that will need to be recorded to be able to be reviewed. There is also the challenge of new types of non-verbal speech, such as digital worlds and items, which will also face some kind of moderation by platforms.[54]

The policy-making process for content moderation in the metaverse is complex and requires collaboration between content moderation partners and clients to continually update policies. Policies should respect the personal space of users while keeping them safe from harmful content or behavior. [55]

[52] https://www2.deloitte.com/us/en/insights/industry/technology/emerging-regulations-in-the-metaverse.html
[53] https://link.springer.com/article/10.1007/s13347-023-00645-4
[54] https://itif.org/publications/2022/04/28/lessons-social-media-creating-safe-metaverse/
[55] https://www.techmahindra.com/en-in/blog/importance-of-policy-making-in-content-moderation/

In summary, the current policies and practices for content moderation on Metaverse platforms are still evolving, and there is little global consensus on how to regulate human behaviors in social experiences. However, some regulations have been put in place in certain jurisdictions, and content moderation is more difficult for platforms in the metaverse than on social media. The policy-making process for content moderation in the metaverse is complex and requires collaboration between content moderation partners and clients to continually update policies.

ii. What are the main challenges and gaps in content moderation in the Metaverse?

The Metaverse presents unique challenges and gaps in content moderation that need to be addressed. Here are some of the main challenges and gaps:

a) **Nuanced safety challenges**: Moderators have to contend with nuanced safety challenges, and there are gaps in the company's understanding of user safety. Traditional moderation tools, such as AI-enabled filters on certain words, don't translate well to real-time immersive environments.[56]

b) **Lack of clear and persistent logs of activity online**: While processes for content moderation are well established and studied, they rely on the existence of clear and persistent logs of activity online. The majority of existing practices address harmful content after they have been posted.[57]

c) **Behaviour monitoring and regulation**: The immersive nature of the Metaverse means that not only content but also behaviors will need to be monitored and regulated. Regulation in other digital environments is often reactive and provides punishments after a violation, but the Metaverse is likely to require incentives for positive behaviour combined with effective mechanisms to report, prevent, and act on negative behaviour.[58]

d) **Lack of global consensus**: There is little global consensus on how to regulate human behaviors in social experiences. As Metaverse platforms become more

[56]https://www.technologyreview.com/2023/04/28/1072393/undercover-content-moderator-polices-the-metaverse/

[57] https://dl.acm.org/doi/fullHtml/10.1145/3544548.3581329

[58] https://www.brookings.edu/articles/a-proactive-approach-toward-addressing-the-challenges-of-the-metaverse/

popular, human moderation will not be feasible at the scale required, and new processes will have to be developed to ensure that content is appropriate

e) **Policy gaps**: Currently, there are policy gaps in content moderation for Metaverse platforms. MUIEs (multi-user immersive experiences) will need to develop their own best practices for moderating this new medium to address these issues.[59]

f) **Balancing privacy with moderation**: Balancing privacy with moderation will be a challenge in the Metaverse. Without policies to prevent abuse, safety in the Metaverse will likely be a barrier to widespread adoption.[60]

In summary, the Metaverse presents unique challenges and gaps in content moderation that need to be addressed. These include nuanced safety challenges, lack of clear and persistent logs of activity online, behaviour monitoring and regulation, lack of global consensus, policy gaps, and balancing privacy with moderation.

iii. What are the best practices and examples of effective content moderation in the Metaverse or other similar spaces?

Effective content moderation is crucial for creating a safe and welcoming environment in the Metaverse or other similar spaces. Here are some best practices and examples of effective content moderation in the Metaverse:

a) **Use a mix of human moderators and automated systems[61]:** Automated systems can help moderate content at scale, but human moderators are still needed to deal with nuanced safety challenges and make judgment calls. Companies must invest in the mental, physical, and emotional health of their content moderation teams.[62]

[59] https://itif.org/publications/2022/02/28/arvr-poses-new-content-moderation-challenges-policymakers-should-address/
[60] https://www.brookings.edu/articles/a-proactive-approach-toward-addressing-the-challenges-of-the-metaverse/
[61] https://itif.org/publications/2022/04/28/lessons-social-media-creating-safe-metaverse/
[62] https://www.telusinternational.com/insights/trust-and-safety/article/future-of-content-moderation

b) **Develop clear community guidelines[6364]**: Clear community guidelines can help users understand what is and is not acceptable behaviour in the Metaverse. Different spaces in the Metaverse may have different community guidelines, and moderators must be trained to enforce them.

c) **Monitor content in real-time[6566]**: Real-time monitoring of user-generated content can help moderators catch problematic behaviour before it becomes widespread. Image, video, and speech are the three types of Metaverse Moderation Services. In real-time, speech may be transcribed and translated. The video content moderation may be transcribed and translated.

d) **Use undercover moderators[67]**: Undercover moderators can help catch bad behaviour without users changing their behaviour because they know they are interacting with a moderator. Moderators must be trained to deal with problematic behaviour and have emotional intelligence to determine whether something is appropriate.

e) **Tailor messages to users**: Moderators must be able to tailor their messages to users depending on their behaviour. Automation could lead to overly broad restrictions and invasive surveillance.

f) **Inform content moderation strategies with learnings[68]**: Brands have a great opportunity to inform their metaverse content moderation strategies with learnings.

In conclusion, effective content moderation in the Metaverse requires a mix of human moderators and automated systems, clear community guidelines, real-time monitoring of user-generated content, undercover moderators, tailored messages to users, addressing privacy concerns, and informing content moderation strategies with learnings.

[63] https://www.linkedin.com/pulse/why-its-easier-succeed-metaverse-moderation-than-you-might-
[64] https://www.technologyreview.com/2023/04/28/1072393/undercover-content-moderator-polices-the-metaverse/
[65] https://www.linkedin.com/pulse/why-its-easier-succeed-metaverse-moderation-than-you-might-
[66] https://mixed-news.com/en/the-metaverse-police-a-vr-content-moderator-shares-his-insights/
[67] https://slate.com/technology/2022/05/metaverse-content-moderation-virtual-reality-bouncers.html
[68]

iv. What are the key principles and values that should guide content moderation in the Metaverse?

a) **Responsibility and ethics**: Building a responsible and ethical Metaverse requires embedding responsibility across two dimensions: trust and human dimensions. Trust includes privacy, security, resilience, and intellectual property rights, while human dimensions include safety, sustainability, inclusion, diversity, accessibility, and well-being.[69]

b) **Safety**: Safety is a key principle that should guide content moderation in the Metaverse. Platforms will need to develop policies to respond to harmful content and protect the free speech of users.[70]

c) **Inclusivity**: Inclusivity is another important value that should guide content moderation in the Metaverse. Platforms should ensure that their policies and practices are designed to be inclusive, diverse, and accessible to all users.[71]

d) **Transparency**: Transparency is essential for building trust between users and platforms. Platforms should be transparent about their content moderation policies and provide clear explanations of their processes for flagging and reporting problematic content.[72]

e) **Collaboration**: Collaboration between content moderation partners and clients is necessary to continually update policies. Platforms should work with their users to develop best practices for moderating this new medium.[73]

f) **Flexibility**: Content moderation practices should be flexible enough to adapt to the unique needs and expectations of individual platforms' users. Platforms should adopt content moderation models that usually include some combination of community guidelines, user reporting, and proactive moderation from both human moderators and machine-learning tools.[74]

[69] https://www.accenture.com/us-en/insights/technology/responsible-metaverse
[70] https://itif.org/publications/2022/02/28/content-moderation-multi-user-immersive-experiences-arvr-and-future-online/
[71] https://www.accenture.com/us-en/insights/technology/responsible-metaverse
[72] https://www.fastcompany.com/90811476/why-content-moderation-could-make-or-break-the-metaverse
[73] https://www.ey.com/en_jp/tmt/seven-key-elements-for-companies-to-develop-metaverse-business
[74] https://itif.org/publications/2022/02/28/content-moderation-multi-user-immersive-experiences-arvr-and-future-online/

g) **Cultural competence**: Content moderation appeals processes require 'cultural competence,' taking into account the diversity of cultures and contexts. Platforms should consider the cultural backgrounds of their users when developing content moderation policies.[75]

In summary, the key principles and values that should guide content moderation in the Metaverse include responsibility and ethics, safety, inclusivity, transparency, collaboration, flexibility, and cultural competence. Platforms should work to embed these principles and values into their content moderation policies and practices to ensure a safe and inclusive Metaverse experience for all users.

v. How can stakeholders collaborate and coordinate on content moderation in the Metaverse?

Stakeholders can collaborate and coordinate on content moderation in the Metaverse in several ways. Here are some examples:

a) **Developing industry standards**: Stakeholders can work together to develop industry standards for content moderation in the Metaverse. These standards can help ensure that all platforms are held to the same level of accountability and that users are protected across all platforms.[76]

b) **Sharing best practices**: Platforms can share best practices for content moderation with each other. This can help ensure that all platforms are using the most effective methods for moderating content and that users are protected across all platforms.[77]

c) **Collaborating on research**: Stakeholders can collaborate on research to better understand the challenges and opportunities of content moderation in the Metaverse. This can help inform the development of effective content moderation policies and practices.[78]

[75] https://www.linkedin.com/pulse/sifting-through-noise-non-standard-content-moderation-roschelle
[76] https://www.fastcompany.com/90811476/why-content-moderation-could-make-or-break-the-metaverse
[77] https://www.technologyreview.com/2023/04/28/1072393/undercover-content-moderator-polices-the-metaverse/
[78] https://itif.org/publications/2022/04/28/lessons-social-media-creating-safe-metaverse/

d) **Investing in technology**: Platforms can invest in technology to improve content moderation in the Metaverse. This can include AI-enabled technologies assisted by human moderators, automated content moderation systems, and AI-powered algorithms for detecting and flagging inappropriate content.[79]

e) **Encouraging user reporting**: Platforms can encourage users to report inappropriate content and behaviors. This can help platforms identify and remove problematic content more quickly and effectively.[80]

f) **Providing training and support**: Platforms can provide training and support to their content moderators. This can help ensure that moderators are equipped with the skills and knowledge they need to effectively moderate content in the Metaverse.[81]

g) **Engaging with users**: Platforms can engage with their users to better understand their needs and concerns around content moderation. This can help platforms develop policies and practices that are more responsive to user needs and concerns.[82]

In summary, stakeholders can collaborate and coordinate on content moderation in the Metaverse by developing industry standards, sharing best practices, collaborating on research, investing in technology, encouraging user reporting, providing training and support, and engaging with users. By working together, stakeholders can help ensure that the Metaverse is a safe and inclusive space for all users.

[79] https://www.cogitotech.com/content-moderation/metaverse-moderation-services/
[80] https://slate.com/technology/2022/05/metaverse-content-moderation-virtual-reality-bouncers.html
[81] https://slate.com/technology/2022/05/metaverse-content-moderation-virtual-reality-bouncers.html
[82] https://about.fb.com/news/2022/12/meta-launches-new-content-moderation-tool/

Q23. Please suggest the modifications required in the existing legal framework with regard to:

i. Establishing mechanisms for identifying and registering IPRs in the metaverse.

ii. Creating a harmonized and balanced approach for protecting and enforcing IPRs in the metaverse, taking into account the interests of both creators and users of virtual goods and services.

iii. Ensuring interoperability and compatibility of IPRs across different virtual environments. Kindly give your response with reasons along with global best practices.

The main IPs being created and utilised on and for the metaverse would include:

1. Copyrights
2. Patents
3. Trademarks

The extant laws covering such IPs in India include the Copyright Act, 1957, the Patents Act, 1970 and the Trademark Act, 1999 (collectively "**IP Laws**"). The need for amendments in the IP Laws would vary depending upon the various technologies utilised and implemented in the metaverse, which includes:

a. Extended Reality (including Virtual Reality, Augmented Reality and Mixed Reality)
b. Artificial Intelligence and Machine Learning
c. Blockchain and NFTs
d. Haptics

(collectively "**Metaverse Technologies**")

We will analyse the existing IP laws and map them against each of the Metaverse Technologies hereinbelow:

A. Copyright

A.1. Extended Reality (XR)

(i) As explained in the consultation paper, XR provides an immersive experience to users to consume content using technologically advanced hardware. Here, it is important to note that it is the 'content' and not the 'experience' that would be the subject matter of copyright.

(ii) Most XR enabled content would include videos, images (still and moving) coupled with sounds. The current copyright regime in India would accord protection to such XR enabled content akin to regular content consumed through televisions, computer systems, handheld devices, film theatres and other mediums of consumption of content.

(iii) The definition of a "cinematograph film" as per Section 2(f) read with the definition of a "visual recording" as per Section 2(xxa) of the Copyright Act, 1957 would be sufficient to cover content published on and distributed through XR enabled technologies and devices.

(iv) Further, the source code of the software XR technologies would be protected a literary works under the Copyright Act, 1957.

Takeaway 1: There is no change required in the copyright law in India with respect to protection and registration of technologies and content created for the purpose of consumption through XR.

(v) It is pertinent to mention that while XR technology is not new, the advancement in affordable hardware and software technology has enabled mass production and mass use of the same. As with any technology which is mass used, it becomes susceptible to misuse.

(vi) Proper due diligence must be maintained by content creators and developers to ensure that third party rights, including IP rights and personality rights, are not violated. The works created and published by them are either: (i) original works; or (ii) duly licensed or acquired from the right holder(s); or (iii) in the public domain.

(vii) Enforcement of IP rights on a centralised metaverse/Web3 platform would be akin to enforcement of rights on the Web2 which is governed by extant laws such as the IP Laws, Information Technology Act, 2000, the intermediary guidelines, and the e-commerce guidelines under the Consumer Protection Act.

(viii) The problem with enforcement may arise on a decentralised metaverse/Web3 platform which are operated by communities rather than juristic entities. While non-

compliance with laws and regulation may be an attraction for both good and bad actors, the platform community should be aware that courts, enforcement authorities, and the government are proactive in blocking 'rogue' platforms in India. A platform may be termed 'rogue' if it primarily hosts infringing content and/or does not comply with the existing laws. This practice has been adopted globally which has led to a decline of dedicated pirate websites. It is, therefore, advisable that developers of decentralised platforms adopt appropriate governance models to protect the community and ensure longevity of the platform.

(ix) Some governance models which can be adopted by such decentralised platforms are: (a) adopting community guidelines and governance policies for the platform including devising effective grievance redressal and takedown mechanisms; (b) adherence with and adoption of the governance policies of the protocol layer or infrastructural layer on which the metaverse platform is built; (c) giving legal character to community driven platforms such as DAOs by incorporating a society or an association; or (d) implementation of blockchain and smart contracts to identify and weed out the infringing content on the platform.

Takeaway 2: Existing laws and methods applied by courts and enforcement agencies for enforcement of copyright on Web2 in India would equally apply to infringement of copyright in Web3/metaverse.

A.2. Artificial Intelligence and Machine Learning (AI and ML)

(i) The interface between AI technologies and copyright is two pronged: (a) input stage i.e. for the training of AI models; and (b) output stage i.e. works generated by or through AI.

Issues at the Input Stage – Text and Data Mining Exceptions

(ii) The issues that have arisen in the global arena at the input stage is largely with respect to text and data mining for the purpose of training effective and accurate AI models. Most AI models are trained on publicly available text and data. However, all publicly available data may not be in the public domain and their reproduction through scraping/mining techniques may be subject to copyright and contractual restrictions. Non-availability of recent data (which would most likely be covered by copyright) would introduce an inherent bias in the AI models thus hampering their accuracy and the resultant user experience.

(iii) This may lead to a situation where Big Tech, which has vast amounts of data at its disposal, take lead in training and commercialising AI models. Further, the developer community could benefit from licensing data from the rightsholders including the Big

Tech, provided that the licensing terms are fair, reasonable, and non-discriminatory (FRAND licensing terms[83]).

(iv) With respect to the scientific research community, educational institutions, and cultural heritage institutions (such as libraries and museums) where licensing requirements and restrictions to text and data mining may become an impediment for innovation for the research community in the AI space. Recognising the need for the research community to be empowered, **the European Union[84]** issued the EU Directive 2019/790 allowing a narrow exception allowing the research community to mine text and data for limited non-commercial purposes.

(v) Countries such as **Japan[85]** and **Singapore[86]**, aiming to be hubs for AI development have introduced broader exceptions for text and data mining where copyrighted content may be mined for very specific commercial purposes including for 'computational data analysis'.

(vi) In the **US**, akin to India, the copyright law does not have any specific exception for text and data mining. However, fair use principles may be applied on a case-to-case basis. The US courts in two separate cases, filed on behalf of a group of artists against Stability[87] and by a group of authors against OpenAI[88], are yet to decide the liability for scraping content for the purpose of AI training without the permission of the rightsholders.

(vii) Although it will be detrimental to the rightsholders if all AI developers (commercial and non-commercial) are given a carte blanche to mine text and data, best practices could be adopted from EU, Japan, and Singapore to balance the rights of content owners while ensuring that developer community is able to rely on accurate data to train AI models and mitigate any biases due to lack of accessibility to data.

(viii) Open-source licensing frameworks could also be adopted for the benefit of the AI development community. FRAND licensing terms (as suggested at point (iii) above) could also be adopted.

Takeaway 3: There is no specific exception under Section 52 of the Copyright Act, 1957 for text and data mining in India. A balanced exception may be

[83] https://link.springer.com/article/10.1007/s40319-022-01255-x
[84] Article 3 to 6 of the EU Directive 2019/790
[85] Article 30-4 of the Japanese Copyright Act
[86] Sections 187, 243 and 244 of the Singapore Copyright Act
[87] Sarah Andersen, et al., v. Stability AI Ltd., et al. [Case No. 23-cv-00201-WHO]
[88] Authors Guild, et al., v. OpenAI Inc., et al. [Case No. No. 1:23-cv-8292]

introduced in the law to ensure that India too becomes a destination for AI development.

Issues at the Output Stage – Authorship/Inventorship, Ownership, and Liability

(ix) An important question that has arisen in the international community surrounds the authorship and ownership of AI generated works. Authorship of an AI generated work may be determined on the basis whether the work created is supervised by a human or is completely unsupervised. A jurisdiction-wise analysis with respect to the same has been discussed below.

(x) India

a. In **India**, as per Section 2(d) of the Copyright Act, 1957 an 'author' refers to a human or a legal person, thus making it restricted towards AI.

b. The Indian Copyright Office is also unsure how to deal with such applications. As reported, in 2020, the copyright office rejected an application which listed AI (RAGHAV) as the sole author for an artwork. However, a second application was filed where a natural person and an AI (again RAGHAV) were named as co-authors for another artwork. The copyright office granted registration in this case. The basis of grant of registration is not clear. The Copyright Office later issued a withdrawal notice one year later. In the withdrawal notice, the Copyright Office shifts the burden on the applicant to 'inform the Copyright Office about the legal status of the AI tool Raghav Artificial Intelligence Painting App'.

(xi) USA

a. In the **US**, AI-generated content is not eligible for copyright protection since it is not created by a human being. However, the US Copyright Office has acknowledged that the creator or owner of an AI system may be eligible for copyright protection.

b. In 2018, the US Copyright Office received an application for a visual work that the applicant described as *"autonomously created by a computer algorithm running on a machine."* The application was denied as it was found that the work contained no human authorship. After a series of administrative appeals, the Office's Review Board issued a final determination affirming that the work could not be registered because it was made *"without any creative contribution from a human actor."*

c. Consistent with the US Copyright Office's policies described, applicants have a duty to disclose the inclusion of AI-generated content in a work submitted for registration and to provide a brief explanation of the human author's contributions to the work.

d. Individuals who use AI technology in creating a work may claim copyright protection for their own contributions to that work including 'prompts'. They must use the standard application, and in it identify the author(s) and provide a brief statement in the "Author Created" field that describes the authorship that was contributed by a human.

e. For example, an applicant who incorporates AI-generated text into a larger textual work should claim the portions of the textual work that is human-authored. And an applicant who creatively arranges the human and non-human content within a work should fill out the "Author Created" field to claim: "Selection, coordination, and arrangement of [describe human-authored content] created by the author and [describe AI content] generated by artificial intelligence." Applicants should not list an AI technology or the company that provided it as an author or co-author simply because they used it when creating their work.

f. In the United States, the case of Naruto v. Slater was significant. In this case, a monkey took a selfie using a photographer's camera, and the photographer claimed copyright ownership of the photo. However, the court ruled that the photographer did not own the copyright since he did not take the photo.

g. Similarly, in 2017, in the case of DABUS, an AI system named DABUS (Device for Autonomous Bootstrapping of Unified Sentience) invented by Dr Stephen Thaler was named as the inventor system that created two new inventions, the patent applications filed in United Kingdom, USA and Europe. The United States Patent and Trademark Office (USPTO) denied the patent application since the inventor was not a natural person. in. However, the same was rejected in all jurisdictions on the account of it not being a legal person as required by most Intellectual Property Rights (IPR) regimes.

h. The USPTO concluded that both applications were incomplete because they lacked a valid inventor. According to the USPTO, the U.S. Patent Act *"limit[s] inventorship to natural persons."* Dr Stephen Thaler, who filed the patents on behalf of his AI system, filed a series of appeals until the case reached the Federal Circuit.

i. On appeal, the Court affirmed the district court's holding that an AI could not be listed as an inventor on a patent application because the Patent Act requires that inventors must be natural persons. The Federal Circuit agreed with the USPTO's conclusion that the Patent Act expressly provides that inventors must be "individuals." Because the Patent Act itself does not define the word "individual," the Federal Circuit relied on the U.S. Supreme Court precedent in Mohamad v. Palestinian Auth., 566 U.S. 449 (2012), which explained that when used *"[a]s a noun, 'individual' ordinarily means a human being, a person."*

(xii) Europe

a. In the European Union, the EU Copyright Directive recognizes that AI-generated content may be eligible for copyright protection if the AI system is considered to be an author. However, this is a controversial issue and there is ongoing debate regarding the definition of an "author" in the context of AI-generated content.

b. The European Commission published the 'Study on Copyright and New Technologies'[89] in an effort to guide policymakers, academics, and other stakeholders on the issues pertaining to copyright and AI, the focus of the second part of the study. The second part was divided into two sections: (1) the input of AI systems; and (2) the output of AI systems.

c. As it pertains to the input, the Study noted that *"the scope of the reproduction right is still in the process of being defined by the European courts, especially when purely technical or intermediate copies are made such as within the process for training an AI algorithm through the analysis of protected elements."*

d. Concerning the output, the Study notes that *"the AI-generated output is not protected under copyright in the absence of human creative choices."* The Study concludes that there is no need for new related rights for the output of AI systems, or additional recognition of protections for an artist's particular style *"unless some significant and recognizable features of a protected work or performance are reproduced in the AI output."*

(xiii) Australia

[89] https://op.europa.eu/en/publication-detail/-/publication/cc293085-a4da-11ec-83e1-01aa75ed71a1/language-en

a. There are no copyright exceptions in the Australian Copyright Act, 1968 for artificial intelligence purposes, such as data scraping or using copyrighted work for machine learning.

b. Moreover, the established definition of the copyright under Australian law favours human artists over AI, as in order for copyright to be established two components must be present: (i) the work has to be original; and (ii) it has to come from an author.

c. Australian precedents have established that the author of a copyrighted work must be human. Two such rulings are: (1) the IceTV Pty Ltd v. Nine Network Australia Pty Ltd (2009) 239 CLR 458, where the High Court underlined that copyrighted works have to be produced by *"an independent human intellectual effort"*; and (2) Telstra Corp Ltd v. Phone Directories Co Pty Ltd [2010] FCAFC 149, where the Full Federal Court ruled that the copyright work must come from a human author.

d. Recently, there has been a groundbreaking, judicial decision upheld by the Australian Federal Court in the Thaler v Commissioner of Patents [2021] FCA 879 through which Judge Beach held that Artificial Intelligence can be recognized as the inventor of patent taking a departure from the position in the US and EU.

(xiv) <u>China</u>

a. China's current copyright law does not provide for non-human ownership of copyright, regardless of whether the work is AI-generated or AI-assisted. This said, it does not follow that copyright in an AI-generated work must by default be owned by a human. While future AI-generated output may constitute works from a copyright law standpoint, these works may be ineligible for copyright protection due to their lack of human authorship.

b. According to their Copyright Law, *"the author of a work is a natural person who creates the work."* Under certain circumstances, a legal person or unincorporated organization may be considered a work's author. There is nothing in the law, however, that would support the proposition that computer systems can be treated as authors for copyright purposes.

c. However, since the definition of 'copyright' includes *"any other rights a copyright owner is entitled to enjoy"*[90], a safeguard is put in place to maintain the relative

[90] Article 10, Item 17 if the Chinese Copyright Act

stability of the law so that it does not need to change whenever a new type of works emerges but also leaves some discretionary power to the judges in judicial practices. This may imply that for AI-generated works, Chinese Copyright Law can assign copyright ownership to the investor, developer, or even the user of the AI system to protect incentives for AI innovation.

d. In the landmark Shenzhen Tencent v. Shanghai Yingxun case, the Nanshan District People's Court considered whether an article written by Tencent's AI software Dreamwriter was entitled to copyright protection. The court found that it was, with copyright vesting in Dreamwriter's developers, not Dreamwriter itself. In its decision, the court noted that *"the arrangement and selection of the creative team in terms of data input, trigger condition setting, template and corpus style choices are intellectual activities that have a direct connection with the specific expression of the article."*

(xv) South Africa

a. In July 2021, the South African Patent Office granted a patent for an invention relating to *"food container based on fractal geometry"* with an Artificial Intelligence (AI) system named "DABUS" (Device for Autonomous Bootstrapping of Unified Sentience) listed as an inventor. This happens to be a world's first, wherein an AI system has been recognized as an inventor.

Takeaway 4: Globally, most jurisdictions prevent AI generated works from being protected under their respective copyright laws primarily due to lack of human authorship. However, owing to growing use of AI in the creation of content, countries such as USA and China are adopting a calibrated and practical approach towards modifying their laws and practices within copyright offices to protect works created using AI as a tool.

Suggestion: Countries can also consider providing a truncated term for protection of AI related works to commensurate for the lack of a creative human contribution to the said works.

A.3. Blockchain and NFTs

Blockchain and NFTs will not require any change in the IP laws as blockchain is merely a new medium of communication and NFTs are merely a new mode of communication. However, blockchain technology has the potential to significantly impact copyright law by offering solutions for content ownership, licensing, and digital rights management.

(i) **Proof of Creation and Ownership**

a. Immutable Records: Blockchain's immutable nature allows creators to timestamp their work, creating an unchangeable record of when the work was created. This timestamp can serve as evidence of ownership in copyright disputes.

b. Proof of Authorship: Using blockchain, creators can establish a clear record of their authorship by storing their work on a blockchain, providing a timestamped, tamper-proof ledger of creation.

(ii) **Smart Contracts and Licensing**

a. **Automated Royalties and Payments:** Smart contracts on blockchain platforms can automate royalty payments to copyright holders when their work is used or accessed. This ensures transparency and efficiency in royalty distribution.

b. **Licensing and Permissions:** Smart contracts can encode licensing terms, specifying how a work can be used. Once agreed upon, these terms are enforced automatically upon fulfilment, ensuring compliance and reducing disputes.

(iii) **Content Distribution and Protection**

a. **Decentralized Distribution:** Blockchain-based platforms can facilitate decentralized content distribution, allowing creators to bypass intermediaries and have more direct interactions with consumers while retaining control over their content.

b. **Anti-piracy Measures:** Some blockchain solutions offer methods to combat piracy by tracking the distribution of copyrighted content, providing better control over unauthorized copying and distribution.

(iv) **Challenges and Considerations**

a. **Regulatory Compliance:** Integration of blockchain with copyright law requires compliance with existing regulations, which might need adjustments to accommodate decentralized technologies.

b. **Privacy Concerns:** Public blockchains store information transparently. Protecting sensitive copyright-related information while ensuring transparency is a challenge.

c. **Standardization and Adoption:** Widespread adoption of blockchain-based copyright solutions requires standardization, interoperability, and acceptance across various industries and legal systems.

B. Patents

Besides the issues of inventorship, ownership, and liability as discussed above, the intersection of the metaverse and patent law introduces a unique set of challenges and opportunities. As the metaverse evolves, there will likely be an increasing number of innovations, technologies, and virtual assets that could be subject to patent protection. Here are a few key points regarding the interface between the metaverse and patent law:

(i) <u>Patentable Innovations in the Metaverse</u>

a. **Virtual Technologies:** Patents could cover inventions related to virtual reality (VR), augmented reality (AR), mixed reality (MR), haptic feedback systems, or immersive experiences within the metaverse.

b. **Virtual Assets and Economies:** Innovations in blockchain, non-fungible tokens (NFTs), decentralized finance (DeFi), and digital asset management systems within the metaverse might be patentable.

c. **AI and Algorithms:** Patents might apply to algorithms, artificial intelligence systems, machine learning models, or other computational innovations powering various aspects of the metaverse.

(ii) <u>Challenges and Considerations</u>

a. **Novelty and Non-obviousness:** To obtain a patent, an invention must be novel and non-obvious. Defining these aspects within the evolving landscape of the metaverse can be complex.

b. **Technical vs. Abstract:** Patent law often requires that inventions are technical in nature rather than abstract ideas. Determining the boundary between the two in the metaverse context could pose challenges.

c. **Global Jurisdiction:** The metaverse operates across borders, raising questions about jurisdiction and the application of patent laws across different countries and legal systems.

d. **Emerging Standards:** Standardization in the metaverse may necessitate patent pools or licensing agreements to ensure interoperability and prevent patent disputes that could hinder innovation.

(iii) **Opportunities**

a. **Innovation Incentives:** Patents can incentivize innovation by granting exclusive rights to inventors, potentially fostering further development within the metaverse.

b. **Monetization and Market Expansion:** Patent holders can monetize their inventions through licensing agreements, collaborations, or by entering new markets within the metaverse economy.

c. **Protection of Virtual Assets:** Patents could provide protection for unique virtual assets, technologies, or methodologies, fostering a more secure environment for creators and developers.

C. Trademarks

Trademark law in the metaverse poses intriguing challenges due to the unique nature of the digital environment and the potential for virtual goods, services, and branding. Here's how trademark law intersects with the metaverse:

(i) **Virtual Goods and Services**

a. **Brand Identity:** Trademarks protect brand names, logos, slogans, and symbols. In the metaverse, businesses may create virtual representations of their trademarks to establish brand identity within digital spaces.

b. **Virtual Assets:** Trademarks might extend to virtual goods, distinguishing them from others in the metaverse. This could include virtual clothing, accessories, or any other digital items associated with a particular brand.

(ii) **Brand Enforcement and Protection**

a. **Policing Infringement:** Trademark holders need to monitor the metaverse for unauthorized use of their trademarks in digital environments. This includes taking action against infringers using trademarks without permission.

b. **Takedown Requests:** Platforms hosting metaverse content might receive requests to remove infringing material or assets that violate trademark rights, similar to enforcement for copyright infringement discussed above.

(iii) **Challenges and Considerations**

a. **Jurisdictional Complexity:** The decentralized and global nature of the metaverse raises jurisdictional issues regarding which laws and regulations apply when trademarks are used or infringed upon in digital spaces.

b. **Unique Trademark Use Cases:** Determining what constitutes trademark use within the metaverse can be challenging. The application of traditional trademark principles to virtual environments might require adaptation or clarification.

c. **Emergence of New Trademarks:** The metaverse may give rise to new types of trademarks related to virtual experiences, assets, or interactions, necessitating the expansion or adaptation of existing trademark laws and classification of goods and services[91].

(iv) **Opportunities and Future Developments**

a. **Innovative Branding Strategies:** Businesses may explore new ways to interact with consumers in the metaverse, utilizing trademarks creatively to enhance brand engagement and recognition.

b. **Collaboration and Standardization:** Developing standardized guidelines or industry practices for trademark use and protection in the metaverse could enhance clarity and consistency across digital platforms.

[91] https://guidelines.euipo.europa.eu/2058843/2065747/trade-mark-guidelines/6-25-downloadable-goods-and-virtual-goods