IAFI response to TRAI Consultation Paper on
Digital Transformation through 5G Ecosystem

Introduction to the ITU-APT Foundation of India (IAFI)

We, the ITU-APT Foundation of India (IAFI), are a registered non-profit and non-political industry association registered under the Cooperative Societies Act of India. IAFI has been recognized by the International Telecommunication Union (ITU), the UN Organization for ICT issues, as an international/ regional Telecommunications organization and has been granted the sector Membership of the ITU Radio Communications Bureau (ITU-R), ITU Development Bureau (ITU-D) and ITU Telecommunication Standardization Bureau (ITU-T). IAFI is also an affiliate member of the APT. IAFI has been working for the last 20 years to encourage the involvement of professionals, corporate, public/private sector industries, R&D organizations, academic institutions, and other agencies in the activities of the ITU and APT.
For more details regarding IAFI, please visit https://www.itu-apt.org/

IAFI Response to TRAI Consultation Paper on Digital Transformation through 5G Ecosystem

IAFI Response:

IAFI welcome the opportunity to respond to the Telecom Regulatory Authority of India's (TRAI) consultation paper on Digital Transformation through 5G Ecosystem (Consultation Paper). Given the rapid advancement of new technologies, particularly in relation to the development of virtual worlds and the metaverse, IAFI believe that the decision to initiate a public dialogue will go a long way in ensuring that such technologies are able to meet their full potential. IAFI along with its partner, Meta are happy to act as a joint contributor to these conversations, to support a transparent, responsible, equitable and collaborative ecosystem for digital transformation. To this end, we have provided our responses and recommendations below.

The Consultation Paper was thoroughly reviewed, and IAFI, in collaboration with its partner, offers our recommendations with the anticipation that they will guide all pertinent ministries and stakeholders toward a shared objective.
It may also be noted that several issues and legal questions posed in the Consultation Paper may not fall within TRAI's regulatory ambit.

Q-1. Is there a need for additional measures to further strengthen the cross-sector collaboration for development and adoption of 5G use cases in India? If answer is yes, please submit your suggestions with reasons and justifications.
Please also provide the best practices and lessons learnt from other countries and India to support your comments.
IAFI Response:

Q-1 Response:

Yes, there is a need for additional measures to further strengthen cross-sector collaboration for the development and adoption of 5G use cases in India. We suggest the following:

1. **Encourage Private 5G Networks Expansion:**
   - Reason: Private 5G networks play a crucial role in fostering innovation and addressing specific industry needs.
   - Justification: By encouraging the expansion of private 5G networks, industries can tailor their connectivity solutions to meet unique requirements, enhancing efficiency and competitiveness.
2. **Facilitate Spectrum Allocation for Private Networks:**
   - Reason: Dedicated spectrum allocation ensures reliable and secure connectivity for private 5G networks.
   - Justification: Allocating spectrum specifically for private networks enhances the quality of service, promotes technological advancements, and attracts investments from various sectors.
3. **Incentivize Industry-Specific Use Cases:**
   - Reason: Offering incentives for the development of industry-specific 5G use cases encourages collaboration and accelerates technology adoption.
   - Justification: Industries are more likely to invest in 5G if they see direct benefits, such as increased productivity, cost savings, and improved services.
4. **Further Strengthen Government-Industry Collaboration:**
   - Reason: The ongoing partnership between the government and mobile operators and local manufacturers have paid rich dividends of fastest 5G rollout.
   - Justification: Leveraging collaborative efforts between the government and private sector promotes innovation and accelerates 5G development.

Best Practices and Lessons Learnt:

- **Germany's Industrial 5G Strategy:** Germany has implemented an industrial 5G strategy, promoting private networks in manufacturing. Germany's success is due to tailoring 5G solutions to specific industry needs fosters innovation and enhances overall economic competitiveness.
- **South Korea's Spectrum Allocation for Enterprises:** - South Korea has allocated spectrum specifically for enterprises to build private 5G networks. Such dedicated spectrum has ensured reliability and security, addressing concerns and promoting widespread adoption.
- **China rapid progress in 5G deployment.** The country has a large market for 5G applications, and investing heavily in use of 5G to promote infrastructure development, including roads, ports, airports and industrial undertakings.

Other suggestions: IAFI believes that implementing additional measures are essential to enhance cross-sector collaboration, thereby fostering the development and adoption of 5G use cases in India. The following measures could be implemented:

1. Raise awareness of 5G, by educating businesses and consumers about the benefits of 5G.
2. Launch a 5G applications fund, to provide financial support to businesses that are developing innovative 5G use cases
3. Establish a national 5G innovation hub, to bring together representatives from government, industry, and academia to collaborate on research, development, and testing of 5G use cases.
4. Create a 5G testing and experimentation platform, to provide a sandbox environment for businesses to develop and test 5G applications.
5. Develop a 5G talent pipeline, involving working with educational institutions to develop training programs for 5G skills.

In conclusion, endorsing the expansion of private 5G networks through dedicated spectrum allocation and incentivizing industry-specific use cases will contribute significantly to the successful development and adoption of 5G in India.

Q-2. Do you anticipate any barriers in development of ecosystem for 5G use cases, which need to be addressed? If yes, please identify those barriers and suggest the possible policy and regulatory interventions including incentives to overcome such barriers.

Please also provide the details of the measures taken by other countries to remove such barriers.

IAFI Response:

Yes, following are some of the potential barriers to the development of the 5G ecosystem in India that need to be addressed:

1. Spectrum Availability and Allocation:

- Barrier: Limited availability of suitable spectrum for 5G deployment, No allocation to captive 5G networks. High Cost of spectrum, particularly in lower and mid bands

- Intervention: Expedite the release of additional spectrum for 5G use and ensure transparent and equitable allocation processes, allocate separate spectrum for industries and enterprises, lower reserved price for auctions and permit spectrum exchange for mobile operators

- International Measure: South Korea and the United States have successfully accelerated 5G deployment by making a substantial amount of spectrum available for commercial and captive use.

2. Infrastructure and Deployment Challenges:

- Barrier: Insufficient infrastructure and deployment challenges, including site acquisition difficulties and right of way issues.

- Intervention: Streamline regulatory processes for site approvals, incentivize infrastructure development, and provide guidance for efficient spectrum utilization.

- International Measure: China has implemented policies to simplify site approval processes, accelerating the deployment of 5G infrastructure.

3. Investment and Funding Constraints:

- Barrier: Financial constraints hindering substantial investments in 5G infrastructure.

- Intervention: Provide financial incentives, tax breaks, and regulatory support to attract private investment in 5G infrastructure.

- International Measure: The European Union has introduced funding programs and incentives to encourage private sector investments in 5G infrastructure.

Details of Measures Taken by Other Countries:

1. South Korea:

- South Korea has implemented a comprehensive 5G strategy, offering financial incentives and regulatory support to telecom operators, encouraging rapid 5G infrastructure development and deployment.

South Korea has implemented a number of government support programs, including a $500 million fund for 5G research and development. The country has also enacted a number of regulatory reforms, such as the allocation of 5G spectrum for private use.

2. United States:

- Measure: The United States has initiated various spectrum auctions, ensuring the availability of ample spectrum for 5G deployment. Additionally, regulatory reforms have simplified infrastructure deployment processes, fostering a conducive environment for 5G development.

Further, United States has implemented a number of regulatory reforms, such as the allocation of 5G spectrum for private use and the streamlining of the 5G application process.

3. China:

- Measure: China has expedited the approval processes for 5G base station sites, reducing bureaucratic hurdles and accelerating the deployment of 5G infrastructure. China has also implemented a number of government support programs, including a $2 billion fund for 5G infrastructure deployment. The country has also made significant progress in developing its own 5G standards.

In conclusion, addressing spectrum availability, streamlining infrastructure deployment, and providing financial incentives are key interventions needed to overcome barriers in the development of the 5G ecosystem in India. Learning from successful measures taken by other countries will be crucial in formulating effective policies for India.

Q-3. What are the policy measures required to create awareness and promote use of 5G technology and its infrastructure so that the citizens including those residing in rural and remote areas may benefit from the 5G use cases and services to create new economic activities and increase employment opportunities and thereby promote economic growth of the country?

IAFI Response:

1. Awareness Campaigns:

- Measure: Launch nationwide awareness campaigns to educate citizens about the benefits of 5G technology.

- Rationale: Building public awareness is crucial to fostering acceptance and understanding of 5G technology, encouraging its adoption across diverse demographics.

2. Inclusive Infrastructure Development:

- Measure: Implement policies that prioritize the expansion of 5G infrastructure to rural and remote areas.

- Rationale: Ensuring inclusive infrastructure development enables citizens in underserved areas to access the economic and social benefits of 5G, promoting equitable growth.

3. Skill Development Programs:

- Measure: Establish skill development initiatives to equip citizens with the necessary expertise to leverage 5G technology.

- Rationale: Enhancing digital literacy and technical skills is essential for maximizing the potential of 5G, creating a workforce capable of driving economic activities.

4. Incentives for Rural Deployment:

- Measure: Introduce financial incentives for telecom operators to invest in 5G infrastructure in rural and remote areas.

- Rationale: Financial incentives will encourage private sector participation in expanding 5G coverage to underserved regions, promoting economic growth and employment opportunities.

5. Public-Private Partnerships:

- Measure: Facilitate collaborations between the government, private sector, and non-profit organizations to jointly promote 5G adoption.

- Rationale: Public-private partnerships can leverage resources and expertise from various sectors to create comprehensive programs that drive awareness and adoption.

Case Studies of Successful Initiatives:

1. Singapore's Digital Readiness Program:

- Initiative: Singapore's government launched the "Digital Readiness Program," offering training and resources to citizens of all ages to enhance their digital skills, fostering widespread adoption of new technologies.

2. Rwanda's Rural Telecommunication Development:

- Initiative: Rwanda has implemented policies to incentivize telecom operators to expand their networks to rural areas, ensuring that citizens in remote regions have access to modern telecommunication services.

3. Australia's Regional Connectivity Program:

- Initiative: Australia's Regional Connectivity Program focuses on improving digital connectivity in regional and remote areas through targeted infrastructure investments, promoting economic development in these regions.

In conclusion, a comprehensive approach involving awareness campaigns, inclusive infrastructure development, skill development programs, incentives for rural deployment, and public-private partnerships will be instrumental in ensuring that all citizens, regardless of their location, can benefit from 5G technology and contribute to the economic growth of the country.

Q.4. What are the policy measures required to promote use of IoT technology and its infrastructure so that the citizens including those residing in rural and remote areas may benefit from these 5G enabled IoT smart applications and services to create new economic activities and increase employment opportunities and thereby promote economic growth of the country?
IAFI Response:

1. IoT Infrastructure Development: Implement policies that prioritize the development of robust IoT infrastructure across urban, rural, and remote areas.

Building a comprehensive IoT infrastructure ensures that citizens from all regions can access and benefit from innovative IoT applications, fostering economic growth.

2. Financial Incentives for IoT Implementation: Introduce financial incentives for businesses and industries to adopt and implement IoT solutions.

Financial incentives will encourage organizations to invest in IoT technologies, leading to the creation of new economic activities and employment opportunities.

3. Skill Development Programs for IoT: Establish skill development initiatives focused on IoT technologies to empower the workforce with the necessary skills.

Developing a skilled workforce capable of working with IoT technologies is crucial for the successful implementation and utilization of IoT applications.

4. Promotion of Smart Agriculture Practices: Introduce policies to promote the adoption of IoT in agriculture, facilitating smart farming practices.

Smart agriculture enhances productivity, reduces resource wastage, and opens new avenues for economic activities and employment in rural areas.

5. Public-Private Partnerships for IoT Projects: Encourage collaborations between the government, private sector, and research institutions to jointly undertake IoT projects.

Public-private partnerships leverage expertise and resources from various sectors, accelerating the deployment of IoT solutions and ensuring widespread access.

6. Expand Broadband Infrastructure - prioritize the expansion of broadband infrastructure, including fiber optic networks, to provide reliable and high-speed internet connectivity to rural and underserved regions. Promoting Tower Infrastructure Sharing, among telecom operators to reduce deployment costs and expand coverage to remote areas.

7. Incentivize IoT Adoption - Financial Incentives, such as subsidies or tax breaks, to encourage businesses and individuals to adopt IoT solutions. Pilot Projects and Demonstrations, showcasing the benefits of IoT applications in various sectors, such as agriculture, healthcare, and education, to create awareness and encourage adoption.

8. Promote Standardization and Interoperability - open Standards and Protocols, to promote the adoption of open standards and protocols for IoT devices and platforms to ensure interoperability and reduce compatibility issues. Testing and Certification Programs, to ensure that IoT devices meet performance, security, and privacy standards.

9. Address Cybersecurity Concerns - strengthen Cyber security Frameworks, robust regulations to protect IoT devices and networks from cyber attacks. Cyber security Awareness and Education, to raise awareness about cyber security risks and educate users on best practices to protect their IoT devices and data.

9. Up-skilling and Training Programs - IoT Skills Training, developing and implementing IoT skills training programs to equip individuals with the necessary competencies to develop, deploy, and manage IoT solutions. Industry-Academia Collaboration, to develop training curricula and certifications aligned with industry demand, ensuring that skilled workers are available for the growing IoT sector.

10. Support for IoT Startups and Entrepreneurs - start-up Incubators and Accelerators, establishing IoT-focused start-up incubators and accelerators to provide funding, mentorship, and access to resources for IoT entrepreneurs. Government Procurement Programs, to encourage the adoption of IoT solutions by government agencies through procurement programs that prioritize innovative IoT-based solutions.

Case Studies of Successful Initiatives:

1. Netherlands' IoT Living Lab: The Netherlands established an IoT Living Lab, bringing together businesses, government, and academia to collaboratively develop and test IoT applications. This initiative has led to the successful implementation of smart city solutions.

2. China's Rural IoT Development: China has initiated programs to implement IoT technologies in rural areas, particularly in agriculture. This has resulted in increased agricultural productivity and the creation of new economic opportunities in these regions.

In conclusion, a comprehensive approach involving IoT infrastructure development, financial incentives, skill development programs, promotion of smart agriculture, and public-private partnerships will be crucial in ensuring that citizens, regardless of their location, can benefit from 5G-enabled IoT applications, fostering economic growth in the country.

Q-5. What initiatives are required to be taken by the Government to spread awareness among the citizens about IoT enabled smart applications? Should the private companies / startups developing these applications need to be engaged in this exercise through some incentivization schemes?

IAFI Response:
To enhance citizen awareness of IoT- enabled smart applications, the government should embark on a comprehensive initiative involving collaboration between government agencies and private companies/start-ups that develop such applications. The following outlines key strategies for implementation.

Government Initiatives:

1. **Public Awareness Campaigns,** to educate citizens about the benefits and potential of IoT-enabled smart applications, highlighting their ability to improve lives and communities.

2. **Demonstration Centers and Showrooms, e**stablishing demonstration centers and showrooms across the country where citizens can experience IoT-enabled smart applications firsthand, fostering understanding and adoption.

3. **Community Workshops and Training Programs,** to provide hands-on training on using IoT-enabled smart applications, empowering citizens to utilize these technologies effectively.

4. **Digital Literacy Programs -** Implement digital literacy programs to bridge the digital knowledge gap and empower citizens to effectively understand and utilize IoT-enabled smart applications.

5. **Collaborations with Media and Influencers,** to disseminate information about IoT-enabled smart applications, reaching a wider audience and enhancing awareness.

Private Sector Engagement and Incentivization:

1. **Partnership with IoT Start-ups and Companies,** to co-develop and implement public awareness campaigns, leveraging their expertise and resources.

2. **Joint Demonstration Projects and Showrooms,** to set up joint demonstration projects and showrooms showcasing the latest IoT-enabled smart applications, providing citizens with real-world experiences.

3. **Targeted Awareness Campaigns in Rural Areas, t**o launch targeted awareness campaigns in rural areas, focusing on the specific needs and challenges of rural communities.

4. **Localized Language Support and Training,** to provide localized language support and training materials for their IoT-enabled smart applications, ensuring accessibility for all citizens.

5. **Incentives for Innovation and Content Creation - p**rovide incentives for private companies to develop innovative IoT-enabled smart applications and create engaging content that promotes understanding and adoption.

Q- 6. Industry 4.0 encompasses Artificial intelligence, Robotics, Big data, and the Internet of things and set to change the nature of jobs.
(a) What measures would you suggest for upskilling the top management and owners of industries?
(b) What measures would you suggest for upskilling the workforce of industries?

(c) What kind of public private partnership models can be adopted for this upskilling task?
Please reply with proper justification and reasons and also by referring to the global best practices in this regard.

IAFI Response:

Industry 4.0, the fourth industrial revolution, can be achieved by the convergence of four important technologies viz Artificial Intelligence, Robotics, Big Data, and the Internet of Things (IoT). On one side, the revolution 4.0 is transforming industries and creating new opportunities, but it also presents challenges, in terms of workforce upskilling and reskilling.

Some measures suggested for upskilling the top management and owners of industries:

(a) Upskilling Top Management and Owners:

1. Executive Education Programs, to encourage top management and owners to participate in executive education programs that focus on Industry 4.0 technologies, their impact on industries, and strategies for adapting to the changing landscape. Industry-Specific Training Courses needs to be arranged on the application of Industry 4.0 technologies in the respective industries, equipping top management with the knowledge to make informed decisions

2. Industry-Academia Collaborations, collaborations between industries and academic institutions to develop and offer customized executive education programs tailored to the specific needs of different industries.

3. Industry Forums and Conferences, to discuss Industry 4.0 trends, allowing top management to stay updated on the latest developments and exchange best practices.

4. Mentorship and Coaching Programs, to connect experienced Industry 4.0 experts with top management, facilitating knowledge transfer and personalized guidance.

(b) Up-skilling the Workforce:

1. Skill Gap Analysis, to identify the specific skills required for Industry 4.0 jobs and compare them to the existing skills of the workforce.

2. Tailored Training Programs, to address the identified skill gaps, providing targeted training on Industry 4.0 technologies and their application in specific job roles.

3. On-the-Job Training and Apprenticeships, to allow workers to learn from experienced professionals while gaining hands-on experience with Industry 4.0 technologies.

4. Online Learning Platforms and Resources, that offer Industry 4.0 training courses, allowing workers to learn at their own pace and convenience.

5. Industry Certifications and Micro-credentials, to encourage workers to pursue industry certifications and micro-credentials in Industry 4.0 technologies, demonstrating their proficiency and enhancing their employability.

(c) Public-Private Partnership Models:

1. Industry-Led Consortiums, to bring together companies, academia, and government agencies to collaborate on upskilling initiatives and share best practices.

2. Co-funded Training Programs, the government and industry partners share the costs of developing and delivering upskilling programs.

3. Skills Voucher Schemes, to provide financial assistance to workers for upskilling courses related to Industry 4.0 technologies.

4.Tax Incentives for Up-skilling, provide tax incentives to companies that invest in upskilling their workforce, encouraging them to prioritize employee development.

Q.7. What are the policy, regulatory and other challenges faced by MSMEs in India in adoption of Industry 4.0. Kindly suggest measures to address these challenges. Provide detailed justification with reasons along with the best practices in other countries.
IAFI Response:

Micro, Small and Medium Enterprises (MSMEs) are the backbone of the Indian economy, contributing significantly in generating employment, economic growth, and social development. However, MSMEs face several challenges in adopting Industry 4.0 technologies.

a. Policy and Regulatory Challenges:

1. **Lack of Clear Policy Framework, specifically addresses the needs of MSMEs in Industry 4.0 adoption. This lack of clarity hinders MSMEs' ability to access funding, navigate regulatory processes, and make informed investment decisions.**

2. **Inadequate Regulatory Support - Streamlining regulatory processes and data privacy frameworks are crucial for encouraging Industry 4.0 adoption.**

3. **Standardization and Interoperability Issues- lack of standardization and interoperability among Industry 4.0 technologies can pose challenges for MSMEs in integrating these technologies into their existing systems and processes.**

b. **Financial and Access Challenges:**

1. **Limited Financial Resources - MSME faces financial constraints that limit their ability to invest in expensive Industry 4.0 technologies and infrastructure.**

2. **Lack of Access to Expertise- MSMEs lack in-house expertise to understand, implement, and maintain Industry 4.0 technologies. Government-supported training programs, industry-academia collaborations, and access to expert consultants can address this challenge.**

3. **Inadequate Infrastructure- rural and remote areas often lack the necessary infrastructure, such as high-speed internet connectivity and reliable power supply, which are essential for the adoption of Industry 4.0 technologies.**

c. **Awareness and Skill Gap Challenges:**

1. **Limited Awareness of Industry 4.0 Benefits, as many MSMEs are not fully aware of the benefits of Industry 4.0, such as improved efficiency, reduced costs, and enhanced customer experience.**

2. **Skill Gap in Workforce - shortage of skilled professionals with expertise in Industry 4.0 technologies among the MSME workforce.**

d. **Measures to Address Challenges:**

1. **Develop a Comprehensive MSME Industry 4.0 Policy - a comprehensive policy framework that outlines clear guidelines, incentives, and support mechanisms for MSMEs to adopt Industry 4.0 technologies.**

2. **Streamline Regulatory Processes to facilitate the adoption of Industry 4.0 technologies by MSMEs. It has to be ensure that data privacy frameworks are aligned with Industry 4.0 requirements.**

3. **Promote Standardization and Interoperability – to encourage the development and adoption of open standards and protocols for Industry 4.0 technologies to ensure interoperability and reduce compatibility issues.**

4. **Providing Financial Support and Subsidies, government-backed funding schemes, subsidies, and tax incentives to make Industry 4.0 technologies more affordable for MSMEs.**

5. **Facilitate Access to Expertise – by establishing knowledge-sharing platforms and collaboration forums between MSMEs, industry experts, and academia to bridge the expertise gap.**

6. **Enhance Infrastructure Development – by developing high-speed internet connectivity, reliable power supply, and digital infrastructure in rural and remote areas to support Industry 4.0 adoption.**

7. **Raise Awareness through Public Campaigns - nationwide public awareness campaigns to educate MSMEs about the benefits, applications, and potential of Industry 4.0 technologies.**

8. **Invest in Skill Development Programs - industry-aligned skill development programs and training initiatives to equip the MSME workforce with the necessary skills to operate and maintain Industry 4.0 technologies.**

Q.8. What additional measures are required to strengthen the National Trust Centre (NTC) framework for complete security testing and certification of IoT devices (hardware as well as software) under DoT / TEC. What modifications in roles and responsibilities are required to make NTC more effective?
Kindly provide your comments with justification in line with the global best practices

IAFI Response:

To enhance the robustness of the National Trust Centre (NTC) framework dedicated to comprehensive security testing and certification of IoT devices, a series of additional measures in roles and responsibilities can be introduced within the ambit of the Department of Telecommunications (DoT) and the Telecommunication Engineering Centre (TEC).

1. **Enhance Testing Capabilities**:

a. Invest in Advanced Testing Infrastructure – NTC must be equipped with advanced testing infrastructure, including sophisticated testing tools, emulation environments, and real-world simulation capabilities, to effectively test a wide range of IoT devices.

b. Expand Testing Scope - to cover all aspects of IoT device security, including vulnerability assessment, penetration testing, secure coding practices, and compliance with relevant security standards.

c. Develop Specialized Testing Expertise – by developing specialized testing teams with expertise in various IoT device platforms, protocols, and security vulnerabilities to ensure comprehensive testing.

2. **Strengthen Certification Process**:

a. Establish Rigorous Certification Criteria - that align with international best practices and industry standards, ensuring that only IoT devices that meet high security standards receive certification.

b. Implement Continuous Monitoring - to track the security posture of certified devices throughout their lifecycle, identifying and addressing any emerging vulnerabilities promptly.

c. Promote Transparency and Traceability - by publishing detailed test results and certification reports, enabling users to make informed decisions.

3. **Enhance Collaboration and Knowledge Sharing**:

a. Collaborate with Industry Experts - partnerships with industry experts, academia, and cybersecurity research organizations to share knowledge, identify emerging threats, and develop new testing methodologies.

b. Foster Information Sharing Platforms - secure information sharing platforms where NTC can collaborate with device manufacturers, security researchers, and CERTs to exchange vulnerability information and facilitate rapid security patching.

c. Participate in International Standards Bodies - active participation in international standards bodies related to IoT security, contributing to the development of global best practices and harmonizing certification requirements.

4. **Strengthen NTC's Role and Responsibilities**:

a. Expand Mandate and Resources - NTC's mandate to include not only testing and certification but also providing cybersecurity guidance, training, and incident response support to IoT device manufacturers and users.

b. Enhance Regulatory Authority - NTC to work as authority to enforce security standards and regulations related to IoT devices, ensuring compliance and protecting consumers from insecure products.

c. Establish a Public Disclosure Policy - a clear public disclosure policy for handling vulnerabilities discovered during testing, enabling timely notification to device manufacturers and users.

Q.9. IoT security challenges and requirements vary significantly across different industry verticals. Is there a need to develop sector-specific IoT security and privacy guidelines?

IAFI Response:

Yes, there is a need to develop sector-specific IoT security and privacy guidelines. Healthcare industry needs to protect sensitive patient data of the patient, while the financial industry needs to protect financial transactions from fraud. Different industry verticals have different security and privacy needs, and a one-size-fits-all approach to IoT security will not be effective.

The development of sector-specific IoT security and privacy guidelines is a complex task and requires involvement of wide range of stakeholders in the development process, including industry representatives, government officials, and security experts.

Developing sector-specific IoT security and privacy guidelines offers a multitude of advantages, as detailed below.

1. Identify and address the specific security and privacy risks that are relevant to each industry vertical.
2. Develop tailored security and privacy controls that are appropriate for each industry vertical.
3. Raise awareness of IoT security and privacy issues among industry stakeholders.
4. Promote the development of secure and privacy-respectful IoT products and services.

Several countries are taking proactive steps to address the security and privacy challenges posed by the Internet of Things (IoT) by developing sector-specific guidelines. The United Kingdom, for instance, has already published comprehensive guidelines for the healthcare, financial, and energy sectors, providing a framework for secure IoT implementation in these critical domains.

Q.10. If answer to Q.9 is yes, is there a need for a common framework and methodology for developing such sector-specific guidelines.

IAFI Response:

Yes, a common framework for sector-specific IoT security and privacy guidelines is essential for creating a secure and trusted IoT ecosystem. It provides a structured approach that can be adapted to different sectors while promoting collaboration, efficiency, and ongoing improvement in the face of evolving security challenges.

A common framework for developing sector-specific IoT security and privacy guidelines should include the following.

a. A definition of the scope of the guidelines.
b. A set of principles that should guide the development of the guidelines.
c. A methodology for identifying and assessing the security and privacy risks associated with IoT devices in each industry vertical.

d. A set of recommended security and privacy controls for each industry vertical.

e. A process for reviewing and updating the guidelines on a regular basis.

The development of a common framework for sector-specific IoT security and privacy guidelines would be a valuable resource for industry stakeholders, government officials, and security experts. It would help to ensure that IoT devices are developed, deployed, and used in a secure and responsible manner.

Q.11. Please suggest regulatory and policy interventions required to ensure privacy of the massive amount of sensitive user data generated by IoT applications specifically in light of the Digital Personal Data Protection Act, 2023.
Kindly provide justifications along with the global best practices.

IAFI Response:
Considering the vast amount of data generated by IoT devices, several regulatory and policy measures need to be implemented to safeguard user privacy in compliance with the Digital Personal Data Protection Act, 2023 (DPDPA). Following measures are to establish clear guidelines, enhance data protection practices, and empower individuals with control over their personal information.

1. Establish Clear Data Collection and Usage Guidelines:

a. **Define Permissible Data Collection – It should be c**learly define the types of data that IoT applications can collect, ensuring that data collection is limited to what is necessary for the intended functionality.

b. **Purpose Specification and Transparency -** IoT applications to explicitly state the purpose for collecting personal data and obtain informed consent from users before data collection.

c. **Data Minimization Principle - P**rinciple of data minimization, to ensure that only the minimum amount of data is collected and retained.

d. **Transparent Data Usage Practices:** Require IoT applications to provide clear and accessible information about how data is being used, including sharing practices and data retention policies.

2. Enhance Data Protection Practices:

a. **Data Encryption and Security -m**andate the use of strong encryption measures to protect personal data both at rest and in transit, preventing unauthorized access and data breaches.

b. **Access Control Mechanisms -** robust access control mechanisms to restrict access to personal data only to authorized individuals and applications, minimizing the risk of unauthorized data exposure.

c. Regular Security Audits and Vulnerability Assessments - IoT application providers to conduct regular security audits and vulnerability assessments to identify and address potential security weaknesses.

d. **Data Breach Notification Requirements -** clear data breach notification requirements, mandating that IoT application providers promptly notify users and relevant authorities in case of data breaches.

3. Empower Users with Control over Their Personal Data:

a. **User Data Access and Control Mechanisms – to p**rovide users with clear and accessible mechanisms to access, review, and correct their data collected by IoT applications.

b. **Data Portability Rights – to g**rant users the right to data portability, enabling them to transfer their data from one IoT application to another in a secure and standardized manner.

c. **Right to Erasure -** allowing users to request the deletion of their personal data from IoT application providers, with exceptions for legal or compliance purposes.

d. **Opt-out Options for Data Collection and Sharing - p**rovide users with clear and easily accessible opt-out options for data collection and sharing, allowing them to control how their personal information is used.

Global Best Practices:

Many countries have successfully instituted robust data protection laws and regulations, setting noteworthy benchmarks for ensuring privacy within the Internet of Things (IoT) ecosystem. Prominent among these are the General Data Protection Regulation (GDPR) within the European Union, the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada, and the Personal Data Protection Law (PDPL) in Singapore. These legislations stand out as exemplars of comprehensive frameworks designed to safeguard individual privacy, providing valuable insights and best practices that can serve as a foundation for guiding similar efforts globally in the evolving landscape of IoT security and privacy.

By adopting similar regulatory and policy measures, India can effectively safeguard the privacy of its citizens in the context of the DPDPA and ensure a responsible and secure IoT ecosystem that respects individual privacy rights.

Q.12. What additional policy and regulatory measures are required to encourage research and development of IoT use cases in various sectors? Is there a need to incentivize startups for research and development of IoT enabled use cases in various industry verticals?

If yes, kindly suggest measures for the same.

IAFI Response:
Additional policy and regulatory measures are required to develop a conducive environment for innovation, to stimulate collaborative efforts, and encourage substantial investment in solutions driven by IoT technologies, in order to create a supportive environment for innovation, foster collaboration, and promote investment in IoT-driven solutions. In order to encourage research and development of IoT use cases in various sectors and incentivize startups, a combination of policy and regulatory measures needs to be implemented.

Policy Measures:

a. **Establish National IoT R&D Strategy -** a comprehensive national IoT R&D strategy that outlines the government's vision, priorities, and funding mechanisms for IoT research and development.

b. **Promote Industry-Academia Partnerships -** collaborations between industry and academia to facilitate knowledge transfer, joint research projects, and the development of industry-relevant IoT solutions.

c. **Create IoT Testing and Experimentation Facilities -** dedicated IoT testing and experimentation facilities where startups and researchers can access infrastructure and resources to develop and test their IoT solutions in real-world environments.

d. **Develop Open Data Platforms and APIs – to** development of open data platforms and APIs that provide access to relevant data sets for IoT research and development, fostering innovation and enabling data-driven solutions.

e. **Encourage Standardization and Interoperability -** adoption of open standards and protocols for IoT devices and platforms to facilitate interoperability and reduce compatibility issues, encouraging broader adoption of IoT solutions.

Regulatory Measures:

a. **Streamline Regulatory Processes – to r**eview and streamline existing regulations related to IoT devices and data privacy to ensure they are not hindering innovation and development.

b. **Establish Clear Regulatory Sandboxes - i**mplement regulatory sandboxes that allow startups and innovators to test and experiment with new IoT technologies and business models in a controlled environment with reduced regulatory burdens.

c. **Promote Regulatory Flexibility for IoT Pilots and Prototypes - p**rovide flexibility in regulatory requirements for IoT pilots and prototypes, allowing for experimentation and refinement of IoT solutions before full-scale deployment.

d. **Encourage Public-Private Collaboration in Regulatory Development - e**ngage industry stakeholders, startups, and academia in the development of IoT regulations to ensure they are aligned with the needs of the ecosystem and promote innovation.

Incentivizing Startups:

a. **Provide Financial Incentives -** such as grants, subsidies, and tax breaks, to startups that are developing innovative and impactful IoT solutions in various industry verticals.

b. **Establish Incubators and Accelerators – developing** IoT incubators and accelerators that provide startups with mentorship, networking opportunities, and access to funding to accelerate their growth and success.

c. **Promote Procurement of IoT Solutions from Startups -** government agencies and public sector organizations to procure IoT solutions from startups, providing them with market access and opportunities for validation.

d. **Launch IoT Innovation Challenges and Competitions -** to encourage startups to develop creative and problem-solving IoT solutions, providing recognition and prizes to foster innovation.

Q.13. What measures should be taken to encourage centres of excellence to handhold startups working in the development of use cases and applications in 5G and beyond technologies? How can the domestic and foreign investors be encouraged to invest for funding the startups for these kinds of development activities?

IAFI Response:
In order to **foster a relationship between established centres of expertise and new startups,** working in the development of use cases and applications in 5G and beyond technologies, and to attract domestic and foreign investors to fund these startups, following measures can be taken.

Measures for Centers of Excellence:

a. **Establish Dedicated 5G and Beyond Innovation Centres - e**stablishing dedicated 5G and beyond innovation centers within universities, research institutions, and industry consortia to provide startups with access to advanced testing infrastructure, expertise, and mentorship.

b. **Develop Tailored Support Programs - d**esign and implement tailored support programs tailored to the specific needs of startups, including technical assistance, business development guidance, and access to funding opportunities.

c. **Foster Collaboration and Knowledge Sharing -** collaboration and knowledge sharing between centers of excellence and startups through workshops, seminars, and joint research projects to foster innovation and accelerate technology transfer.

d. **Provide Prototype Development Funding -** funding to startups for the development of prototypes and proof-of-concept demonstrations, allowing them to showcase the viability of their 5G and beyond solutions.

e. **Promote Open Innovation Platforms -** open innovation platforms that connect startups with potential partners, investors, and customers, facilitating collaboration and market access.

<u>Encouraging Domestic and Foreign Investors</u>:

a. **Create Specialized Investment Funds -** creation of specialized investment funds focused on 5G and beyond startups, providing access to capital for early-stage and high-potential companies.

b. **Provide Tax Incentives for Investors -** for investors who invest in 5G and beyond startups to stimulate private sector participation.

c. **Government-Industry Co-investment Programs -** government-industry co-investment programs that match private sector investments in 5G and beyond startups, sharing the risk and reducing financial barriers for investors.

d. **Promote Investment Opportunities -** promote investment opportunities in 5G and beyond startups at industry events, conferences, and international roadshows to attract global investors.

e. **Streamline Regulatory Processes for Foreign Investors -** streamline regulatory processes for foreign investors investing in 5G and beyond startups, reducing administrative burdens and enhancing investor confidence.

Q.14. Whether there is a need to make changes in relevant laws to handle various issues, including liability regime and effective mechanism for redressal and compensation in case of accidents, damages, or malfunctions involving IoT, drones, or robotic systems. If yes, give detailed suggestions.

IAFI Response:

There is a need to make changes in relevant laws to handle various issues, including liability regime and effective mechanism for redressal and compensation in case of accidents, damages, or malfunctions involving IoT, drones, or robotic systems. The following are detailed suggestions for making changes in relevant laws.

a. Define Clear Liability Standards, establishing clear and well-defined liability standards for manufacturers, operators, and users of IoT devices, drones, and robotic systems. This includes specifying responsibilities for each party in the event of accidents or malfunctions.
b. Product Liability Regulations - Implement or update product liability regulations to hold manufacturers accountable for the safety and security of their IoT, drone, or robotic products.
c. Insurance Requirements - mandate insurance requirements for IoT, drone, and robotic system operators to ensure that there is financial coverage in case of accidents or damages. This can provide a mechanism for compensation without solely relying on legal proceedings.
d. Privacy and Data Protection Laws - strengthen privacy and data protection laws to address the unique challenges presented by IoT devices. Ensure that data collected by these devices is handled responsibly, and users are adequately informed about how their data is being used.
e. Regulatory Oversight - establish or enhance regulatory bodies with expertise in IoT, drones, and robotic systems to oversee compliance, investigate incidents, and enforce safety standards. These bodies should have the authority to impose penalties for non-compliance.
f. International Standards Collaboration - encourage collaboration with international organizations to develop and adopt standardized regulations for IoT, drones, and robotic systems. Consistency in standards can facilitate global interoperability and streamline legal processes.
g. Redressal Mechanism - develop an effective redressal mechanism for individuals or entities affected by accidents, damages, or malfunctions involving IoT, drones, or robotic systems. This may include alternative dispute resolution mechanisms to expedite the resolution process.
h. Public Awareness and Education - Implement public awareness and education campaigns to inform users, operators, and manufacturers about their rights, responsibilities, and the potential risks associated with these technologies. This can contribute to responsible use and better compliance.
i. Continuous Legal Review - establish a framework for continuous legal review to keep pace with the rapid evolution of technology. Regularly assess and update laws to address emerging challenges and technological advancements in IoT, drones, and robotic systems.
j. Collaboration with Industry Stakeholders - foster collaboration with industry stakeholders, including manufacturers, technology developers, and user communities, to gather insights and ensure that regulations are practical, effective, and adaptable to technological advancements.
k. Emergency Response Protocols -develop and integrate emergency response protocols specifically tailored for accidents or incidents involving IoT, drones, and robotic systems to minimize harm and streamline recovery efforts.

Q.15. Is there a need to have a separate security mechanism for Multiaccess Edge Computing (MEC)? If yes, please give your inputs and suggestions with regard to policies, rules, regulations and guidelines.
There is a need for a separate security mechanism for Multiaccess Edge Computing (MEC). MEC is a decentralized computing architecture where computation is performed closer to the edge of the network, bringing numerous benefits in terms of reduced latency and improved performance. However, the distributed nature of MEC also introduces new security challenges that need to be addressed. Following are some inputs and suggestions regarding policies, rules, regulations, and guidelines for securing Multiaccess Edge Computing.

a. Access Control Policies, implementing strict access control policies to regulate access to MEC resources. Ensure that only authorized entities, devices, or applications have access to the computing resources at the edge. This involves identity verification, authentication, and authorization mechanisms.
b. Data Encryption - enforce robust encryption mechanisms for data transmitted and processed at the edge. This includes securing communication channels and data storage to protect sensitive information from unauthorized access or interception.
c. Secure APIs and Interfaces - establishing secure Application Programming Interfaces (APIs) and interfaces for communication between devices, applications, and the MEC infrastructure. This helps prevent vulnerabilities and ensures that interactions are secure and well-defined.
d. Network Security - implement network security measures to safeguard MEC deployments from potential threats. This involves intrusion detection and prevention systems, firewalls, and continuous monitoring of network traffic to identify and mitigate suspicious activities.
e. Device Security – to ensure the security of edge devices connected to the MEC infrastructure. This includes implementing security measures on IoT devices, sensors, and other edge devices to prevent unauthorized access and potential exploitation.
f. Incident Response and Recovery – to develop and document incident response and recovery plans specific to MEC. In the event of a security incident, having a well-defined plan helps in minimizing the impact, identifying the source of the breach, and facilitating a swift recovery.
g. Compliance with Data Protection Regulations – to ensure compliance with data protection regulations, such as GDPR (General Data Protection Regulation) and other regional or industry-specific laws. Define policies for data handling, storage, and processing that align with regulatory requirements.
h. Regular Security Audits and Assessments – to conduct regular security audits and assessments of the MEC infrastructure to identify and address potential vulnerabilities. This proactive approach helps in identifying security gaps and implementing timely corrective measures.
i. Collaboration with Industry Standards -to align security practices with industry standards and best practices. Collaborate with relevant standards bodies and organizations to ensure that MEC security mechanisms adhere to widely accepted guidelines.

j. User Education and Awareness - educate users, developers, and administrators about security best practices specific to MEC. Promote awareness of potential threats, vulnerabilities, and the importance of following security guidelines in the development and deployment of MEC applications.

k. Regulatory Oversight - establish or enhance regulatory oversight specific to MEC security. This could involve defining regulatory frameworks that mandate security standards and periodic assessments for MEC deployments.

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?

RESPONSE:

Generating awareness and conceptualising application of core technologies of metaverse (viz. augmented reality, virtual reality and mixed reality) for the larger public good are likely to lead to more diverse and widespread adoption, as well as greater opportunities to drive innovation. Policymakers should leverage the resources of industry participants and civil society in its efforts to generate awareness, build capacity, and ensure democratic access to the metaverse.

Certain key policy measures may be considered in this regard:

(a) *Awareness and Accessibility*: Given that the metaverse is still at a nascent stage of development and adoption, it is unknown to a large section of the population. The growth of the metaverse should be accompanied by efforts to educate companies, consumers, and policymakers. The government, through collaborations and partnerships with industry, think tanks, academia, civil society organisations, should fund, facilitate and raise in awareness through campaigns and exhibitions to demonstrate best practices within the industry and to make the public aware of new and existing use cases, how to use the metaverse, and how it may benefit them, and how to protect themselves from potential harms. Industry leaders in other sectors (particularly, non-digital sectors) must also be made aware of the potential of metaverse applications, to enable widespread adoption.

A diverse and relevant set of use cases is a sure shot way to promote access and awareness – especially with India's young population – and India's experiments with Unified Payment Interface and Digital Public Infrastructure initiatives are a clear indicator of this. Metaverse products and virtual worlds must also account for the diverse linguistic, cultural, and socio-economic backgrounds of the citizens of Bharat. Catering to rural and semi-urban populations in particular is critical to ensure that they are encouraged to access and use services that may be provided to them through the metaverse. Large technology companies (with their advanced technology capabilities) in collaboration with SMEs and start-ups (with their knowledge of local contexts) will play a crucial role in developing metaverse use cases for Bharat to ensure that such diverse needs are met. Investment in developing talent and incubating new use cases is also critical in this regard, and policymakers can consider creating a dedicated fund for metaverse use cases which cater to rural populations or other unserved communities.

Accessibility doesn't just mean access to the technology. It also means providing opportunities and solutions for people with disabilities. There are already a suite of applications that are benefiting people with disabilities, including speech to text, and hand and eye tracking. These are a few examples of applications that make the technology more approachable and beneficial for those with disabilities.

(b) *Skilling for the metaverse*: Increasing innovation in the metaverse must also be accompanied by upskilling of the Indian workforce to be able to meaningfully participate in the growth of the industry. There exists significant opportunities for large-scale employment, given the advent of new job profiles such as metaverse architects, virtual event planners, AR/VR Software Engineers, and more.

Initiatives must be introduced to create readiness for a metaverse-centric technology landscape, which would prepare the individuals for the complexities as well as the advantages metaverse brings with itself. One of the most effective ways to build readiness for emerging technologies essential for metaverse is to revise the present educational curriculum (both at school and college level) to ensure that it is updated to meet the needs of emerging technologies like AR, VR,MR and Artificial Intelligence. This could include introducing internship and skill-development programmes at the school and college level. As part of these programmes, students can gain the necessary hands-on experience and practical learning to improve their employability and industry readiness.

Besides changes in curricula and skill development programmes, there is a need to create awareness about the future of jobs in educational institutions. Opportunities in XR technologies should be brought to the notice of parents and students to promote greater uptake of such career paths. The focus should be to design jobs and career pathways based on skills and experience, and not educational degrees.

Given that a large number of reputable educational institutions in India are funded and operated by government bodies, India has the opportunity to introduce a strong future-led, innovation-focused curriculum. Policymakers can also take the lead in facilitating collaboration between educational institutions and industry players to assess the existing skills gap and co-design roadmaps to adapt existing programs and strengthen industry-university cooperation. Several companies[1] have already begun investing in programs to skill students and educators in new technologies, as well as to upskill those presently engaged in allied industries, such as investing in creators to help them develop skills in AR, VR and immersive media. Existing programs for upskilling and reskilling in emerging technologies should be strengthened and expanded with increasing industry participation.

(c) *Integration with existing systems*: Significant value can be derived from the application of the metaverse in existing digital and physical ecosystems. Policymakers and implementing entities/agencies should work with industry stakeholders and developers to determine how best to integrate these technologies into existing IT systems. Through a combination of private sector expertise in metaverse deployment and the mandate of the public sector to ensure service delivery to the last-mile, the metaverse can play an increasingly critical role in the lives of Indians living in remote and rural areas. Some examples of use cases for potential collaboration have been indicated below:

(d) Training: The ability to conduct remote skilling through the metaverse eliminates the need for citizens in more rural areas to travel to larger cities to receive training, and also requires less infrastructure (physical space, equipment). With India expected to have 1 billion smartphone users by the end of 2026, enabling citizens to access such online spaces through their smartphones would additionally catalyse such programs[2]. To enable such use cases, policymakers should consider integrating metaverse technology developed by the industry into existing skill development programs.

- E-governance: Citizen services can be provided remotely through the metaverse, enabling rural citizens to access a plethora of services which may be currently difficult to access. Physical requirements of document submission, in-person verification and inspection to avail government services or benefits can be eliminated through the metaverse.

[1] https://timesofindia.indiatimes.com/education/news/cbse-to-introduce-ar-and-vr-under-emerging-knowledge-domain/articleshow/88527846.cms?pcode=461; https://economictimes.indiatimes.com/tech/technology/tech-mahindra-mahindra-university-to-set-up-lab-for-metaverse-quantum-computing/articleshow/93075011.cms?from=mdr

[2] https://www.businesstoday.in/technology/story/india-to-have-1-bn-smartphone-users-by-2026-deloitte-study-323519-2022-02-22

- Tourism: Through the virtual world, it's possible for tourists to explore a destination before they arrive. Tourism departments and district officials in India can utilize metaverse tourism to be able to market and brand rural destinations for tourists, providing a boost to the local economy.

(e) Adoption of XR in government applications to promote innovation and affordability

- XR technologies have the potential to revolutionize the operation of government agencies, improve decision making, and enhance delivery of public services. Notable use cases include transformation of citizen engagement, training at scale, enhancement of urban planning and promotion of tourism.
- As government agencies in India increase investment in XR infrastructure and R&D, it will make technologies affordable, attract companies, foster entrepreneurship, and support the growth of XR-related industries in India. For instance, promoting the use of XR in skilling, tourism, education and training, will help expand the demand for these technologies.
- It is imperative that all Indian government departments stay at the forefront of technological advancements and contribute to the creation of a thriving XR ecosystem.

(f) *Access to digital infrastructure*

- *High-speed Internet:* The most important part of setting up a metaverse friendly technological infrastructure is to ensure easy access to high-speed internet. High speed internet as a foundational component can be achieved by investing and focusing on building necessary network frameworks which support 5G, while supporting hotspot as public access points for the population's wide use. Recently, the government introduced a high-speed internet project focusing on 6.4 lakh villages in India under the BharatNet initiative[3], with an aim to provide seamless connectivity to the rural areas. While the program is in its initial stages[4], and the government seeks to expand it to the national level, we recommend integrating 5G technology as well as collaborating with telecom players in order to make the implementation of this initiative more effective.
- *Community Centers:* Since in rural areas the general community at an individual level will not have the financial wherewithal to seek access to the digital infrastructure and hardware required to access the metaverse, the government can encourage setting up of digital infrastructure in the form of community centers, which are open for everyone's access. For this purpose, funds available to discharge corporate social responsibility ('CSR') obligations may be deployed. Setting up community centers equipped with high-speed internet, computers with adequate specifications can help bridge the digital divide and metaverse supporting hardware like AR/VR headsets.[7] These centers can serve as hubs for digital literacy training, metaverse awareness programs, and skill development workshops. The educational institutions in rural areas, i.e., K-12 schools as well as colleges and universities can be used as centers to run workshops and educational programs using the metaverse. Such workshops and programs can be on varied topics, and the awareness regarding metaverse. Additionally, technological workshops may be conducted with a focus on metaverse, which also impart knowledge about the various use cases of various metaverse tools[8] in different industries as well as privacy and security risk mitigation measures.
-

(g) *Ease* entry barriers for hardware import and incentivize manufacturing in India

- Lack of affordable hardware in India impacts the ability of the Indian ecosystem to reap the benefits of the metaverse economy and underlying futuristic technologies. Many companies are working to make XR devices more affordable over time, but there are several things the government could consider to do now that would have an immediate effect on the price of devices, including lowering tariffs.

[3] https://www.news18.com/tech/high-speed-internet-in-rural-india-big-broadband-plan-gets-cabinet-nod-for-connections-in-6-4-lakh-villages-8513821.html

[4] https://usof.gov.in/en/bharatnet-project

- Easing out the requirement of multiple certifications for selling devices in India could be explored. Presently, testing and certification for telecom and related IT equipment is broadly under the purview of several agencies across different ministries. These include the Bureau of Indian Standards and the Telecommunication Engineering Centre, which administers the Mandatory Testing and Certificate of Telecom Equipment (MTCTE) requirements. Due to this complex administrative structure, it is likely that certain types of devices like VR/AR devices would have to adhere to multiple standards, testing and certification requirements. Harmonizing the testing and certification functions will ensure that the overlaps between different administrative agencies is limited. For example, DOT in consultation with MeitY has exempted products like mobile phones, smart watch from the ambit of MTCTE regime[5]. Further, implementation of regulatory sandboxes can also be one of the ways in addressing entry barriers for specific use cases.
- Additionally, inclusion of XR technology and related products in the Production Linked Incentive (PLI) scheme and other incentives in the form of tax benefits to attract XR related hardware manufacturers to the country can also be considered.

Q.17. Whether there is a need to develop a regulatory framework for the responsible development and use of Metaverse? If yes, kindly suggest how this framework will address the following issues:
i. How can users control their personal information and identity in the metaverse?
ii. How can users protect themselves from cyberattacks, harassment and manipulation in the metaverse?
iii. How can users trust the content and services they access 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?

RESPONSE:

Regulation often lags technological developments. One way to make regulation future proof is to make it technology agnostic. Technologies like the metaverse are at a very early stage of development. In many cases, the metaverse looks to model the real world, and as such may see the similar interactions, transactions and activities that we see in the real world. In this context, it is important to view the metaverse within the existing regulatory framework first, to assess whether regulations that govern real world actions would be effective in regulating similar actions carried out in the metaverse.

The metaverse does not exist in a regulatory vacuum, with several technology neutrality laws in the current Indian legislative and regulatory framework which adequately address issues in connection with the metaverse or relating to the development and use of metaverse. We therefore do not see any requirement for the development of a regulatory framework to specifically govern the responsible development and use of metaverse. This is an approach being considered in various other global jurisdictions. Most countries are not looking to introduce metaverse-specific legal-framework, with jurisdictions like the EU reporting that its existing legal framework is robust and future-oriented enough to apply to several aspects of the development of virtual worlds[6]. In addition to legislation, voluntary codes and standards set by global industry alliances are also effective in regulating the metaverse. The indicative list below demonstrates the adequacy of existing laws, regulations, standards, and guidelines that govern the development and use of metaverse.

[5] https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1821530

[6] European Commission, An EU initiative on Web 4.0 and virtual worlds: a head start in the next technological transition (September, 2023), accessible at < https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3718 >

(a) *Devices:* Several laws and regulatory frameworks in India including telecommunication laws such as the Wireless Telegraphy (Possession) Rules, 1965 and certificatory frameworks such as the Mandatory Testing and Certification of Telecom Equipment (MTCTE) regime, Electronics and Information Technology Goods (Requirements for Compulsory Registration) Order, 2021, impose mandatory licenses, certification and testing requirements for various devices and equipment (for example, AR/VR headsets) that may be used to access and use the metaverse. This framework dictates specifications and prescribes technical configuration standards for the development of various emerging technologies used to access metaverse.

(b) *Control over personal information and identity:* The new data protection regime proposed to come into force in India (i.e., the Digital Personal Data Protection Act, 2023 (**DPDP Act**)) is a comprehensive and robust regulation, which introduces various mechanisms to provide users with autonomy over their personal data. As such, users will now have greater control over the data they share with entities to sign up to the metaverse, as well as any personal data they may share during the course of their use of the metaverse. The DPDP Act provides users with various rights including the right to access and right to correction and erasure in connection with their personal data which would enable users in the metaverse to assert control over how their personal information and various identities are featured in the metaverse. For instance, the principles[7] outlined in the DPDP Act technology neutral should be applied to metaverse as well.

- **Lawfulness, fairness and transparency:** Users should be provided all the information with transparency and also have the tools to manage consent required for any features and services, such that they are always in control of both (i) the nature of data collected; and (ii) the purpose of such data collection. This can be also incorporated in the design of devices such that people can switch off sensors, cameras, or by providing easily accessible options on dashboards.
- **Limitations on purposes of collection, processing, and storage:** The personal data should be used only for the purposes for which it was collected.
- **Data minimization**: The principle of data minimization is an important pillar to ensure that online environments do not automatically become risky environments by excessive collection and sharing indiscriminate amounts of data. Users should be able to exercise choice over how personal data is used and how to personalize their experiences.
- **Accuracy:** Reasonable effort should be taken to ensure that the personal data is accurate and kept up to date.
- **Data storage limits:** Data should not be stored perpetually by default. The storage should be limited to such duration as is necessary for the stated purpose for which personal data was collected.
- **Privacy by design:** Privacy by design can be a method of achieving both data minimization as well as data security. For example, certain types of data, a device collects information regarding a user's immediate surroundings (such as their living room) to indicate acceptable boundaries for physical movement, such data may not be transferred outside the device if such data is not required for any additional purpose. Privacy by design[8] principles can also be helpful to ensure bystander privacy, such that faces of bystanders are automatically blurred by the headset/glasses, or the use of light signaling.
- **Accountability:** The person who decides the purpose and means of processing of personal data should be accountable for processing of data.

Extant information technology and cybersecurity laws read with data protection laws in India also govern a multitude of cyber incidents including identity theft, data breaches etc., which would empower users in the metaverse to seek redressal and shield themselves against cyber-attacks or

[7] https://www.meity.gov.in/writereaddata/files/Explanatory%20Note-%20The%20Digital%20Personal%20Data%20Protection%20Bill%2C%202022.pdf

[8] https://www.meta.com/blog/quest/meta-quest-pro-privacy/?utm_source=www.google.com&utm_medium=oculusredirect; https://newsroom.snap.com/privacy-by-design; https://learn.microsoft.com/en-us/hololens/hololens2-privacy
;

threats to their identity.

There is also considerable international guidance and standards on the use of user data, which serve to govern the activities of operators through the adoption of responsible and protective practices across the data collection and processing chain within the metaverse, to reinforce user safety and individual privacy. For instance, the Metaverse Standards Forum has a dedicated working group on Privacy, Cybersecurity and Identity which develops standards and technical frameworks across jurisdictions and metaverse use cases.

(c) *Payments*: The Blockchain-enabled tools might help support digital payment processes, underpin commerce by tracking ownership of a piece of digital art an artist wants to sell in the metaverse. However, this is only one of the many ways in which digital payments or goods can exist in the metaverse The present payment mechanisms involving digital fiat currency can also enable purchase of digital assets, and serve the overall metaverse ecosystem. There are already many examples today of people buying and selling digital goods with fiat currency like in-gaming coins, eBooks, event or experience tickets, music and audio files and digital art. Hence, several regulations, directions, schemes and notifications implemented by the Reserve Bank of India (**RBI**) offer adequate recourse to individuals in relation to any payments made by them. These would continue to apply to any payments made to avail services or make purchases within the metaverse using regulated payment methods. For instance, the Banking Ombudsman Scheme, 2006 allows any person who has a grievance against a bank on specific grounds such as non-payment or inordinate delay in payment, failure to provide or delay in providing a banking facility, unauthorized electronic payments or funds transfer etc., to make a complaint to the Banking Ombudsman. While the need to regulate other payment systems in the metaverse (such as those made on the blockchain) may need to be separately assessed, it should be noted that the metaverse broadly operates within the scope of existing payment regulations – and it should not be conflated with the regulation of Web 3.0.

(d) *User Safety and trust:* Various acts that may jeopardise user safety are regulated under criminal laws. For instance, the Indian Penal Code, 1860 (**IPC**) penalises the distribution and circulation of obscene material, defamatory content or content that causes disharmony or feelings of enmity or hatred or ill-will between specific groups of members. This serves to strengthen metaverse users' trust in the content they access within metaverse. The IPC further penalises theft, dishonest and fraudulent concealment and destruction of property which would equally apply to online activities. Various laws on content moderation also serve to protect users in the metaverse, as further described in our response to Question 21. Additionally, the Indian Computer Emergency Response Team has also been set up to prevent, forecast and coordinate responses to a variety of cyber incidents which may affect user safety online.

With respect to children's safety, the (Indian) Protection of Children from Sexual Offences (**POCSO**) Act, 2012 prescribes punishment for the use of a child in pornographic material, thereby ensuring that the content accessible in the metaverse is not obscene. Information technology laws also specifically prohibit the handling of any sexually explicit electronic material relating to children. Similarly, the DPDP Act imposes certain restrictions on entities that process children's data such as prohibiting them from undertaking any processing that is likely to have a detrimental effect on the well-being of a child and tracking, monitoring the behaviour of, or directing targeted advertisements at children. These regulations ensure that the content and services that children may access in the metaverse are strictly regulated. Recommendations issued by international agencies are also relevant and can act as voluntary guidance for operating entities. For instance, the United Nations Children's Fund has listed various recommendations in its rapid analysis report titled '*The Metaverse, Extended Reality and Children*'.

The (Indian) Consumer Protection Act, 2019 (**CPA**) governs the marketing, sale and purchase of goods and services in India in order to safeguard the interest of consumers. A specialized central authority created under the CPA is empowered to regulate illegal conduct and consumer harm including certain unfair trade practices such as making false representations about the standard, quality, characteristics, uses or benefits of services, giving warranties/guarantees that are misleading etc. Such provisions under law would ensure users in the metaverse are protected against any deficient digital services and any technical issues with digital assets.

Further, as per the presentation made by Hon'ble Minister of State for Electronics and Information Technology, Mr. Rajeev Chandrashekhar on the proposed DIA (available here), the government is proposing a framework to ensure an open, safe and trusted internet with accountability for platforms providing digital services. We agree with the approach of the government in wanting to avoid a prescriptive law. A principle-based law will encourage innovation while ensuring safety and security.

While, the proposed Digital India Bill, will outline a regulatory framework to enable and safeguard the development of emerging technologies and address the consequent risks, following are some of the measures recommended by various experts and studies:

- To ensure mental safety, features which allow users to block, mute, and report violations are the baseline tools which should be incorporated in the technologies built for accessing Metaverse. Additionally, there would be requirements for ensuring the report of abuse, blocking certain users, setting virtual buffers, and placing appropriate privacy controls.
- Features such as personal boundary which enables creation of distances when interacting in VR is one of critical features to provide users more control and address safety issues.
- To ensure physical safety of users, wearables could enable creation of a pre-established boundary or space in which the user can move once a headset is on. To address ergonomics of the wearables and ensure user comfort investment R&D is needed to re-design the technology.
- Developers should regularly update their XR products and standards for using them with physical and mental safety in mind.
- Safeguarding vulnerable data via encryption, auto deleting data that is no longer needed are some of the ways to ensure security of the data.

(e) *System Security:* The DPDP Act requires entities that handle personal data to implement technical and organisational measures and take reasonable security measures to prevent personal data breaches. While yet to be clarified, such measures may involve implementing data retention standard operating procedures, a notice and consent logging mechanism, encryption etc. International cybersecurity standards can also be relied upon to determine what security measures should be adopted in the metaverse. For instance, the National Institute of Standards and Technology (**NIST**) released standards designed for organizations to manage their privacy and cybersecurity risks, which ensures security-by-design in metaverse development.

We recognise that the metaverse is a new technology and may therefore give rise to unforeseen risks as it continues to develop, and as new use cases are discovered. It is proposed that such risks be explored on a case-by-case basis through a multi-stakeholder approach, with participation from policymakers, public agencies, industry, developers, academia, consumers and civil society. This may take the form of consultations, which are already extensively carried out by various regulators in India to seek public opinion on upcoming regulatory issues. Multi-stakeholder committees and task forces may also be set up, with wide representation. We note that the TRAI has recommended the creation of such bodies on issues of net neutrality and traffic management. A similar body can be considered with respect to Metaverse governance and can be tasked with assessing unforeseen risks arising from the growth of metaverse technologies and work together to determine appropriate policy responses and testing out their findings through the use of sandboxes.

Globally, similar programs like the Metaverse Initiative at the World Economic Forum have been introduced, which brings together over 150 partners across industries and geographies from the private sector, civil society, academia and policy (such as Sony, Stanford University, Meta, Interpol, Deutsch Bank, United Nations Office of Counter Terrorism, the Singapore Government etc.,) to define the parameters of an economically viable, interoperable, safe and inclusive Metaverse

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.

RESPONSE:

The metaverse creates an independent market for new technology products and services, while also serving to enhance and digitally transform existing markets. The creation of new products and services requires a supportive environment for research, experimentation, innovation, value creation and constant development. Given the potential complexities of new technologies, ecosystems such as regulatory sandboxes are ideal to allow metaverse developers to offer products to limited numbers of consumers in a more controlled environment or to engage in experimental governance programs. As opposed to a prescriptive technology-based regulation, regulatory sandboxes allow policymakers to assess potential risks and benefits of a new technology, while allowing industry participants the flexibility to reiterate as required. Experimental ecosystems also enable start-ups and small businesses to test products and gain an early advantage in the market. Jurisdictions globally are looking to regulatory sandboxes to support metaverse innovation. For instance, the EU plans to promote the use of virtual worlds regulatory sandboxes by its Member States. Reports commissioned by the South Korean government also recommend creating regulatory sandboxes to test metaverse applications in games[9]. The Innovation License introduced by the Bahraini Telecommunications Regulatory Authority also encourages development and deployment through testing and trial of new wireless technologies and services[10]. In India, the Government of Telangana has set up a regulatory sandbox for Web 3.0 for innovation in various fields including metaverse[11]. It is recommended that more such initiatives be encouraged and introduced to enable active industry participation in the growth of this industry.

Centres of Excellence (**CoEs**) are perfectly positioned to facilitate these ecosystems in India, as they serve as a platform to bring together the public and private sector to drive co-creation, problem-solving, nurturing innovation and disseminating best practices. We note that some public-private partnerships have been announced towards the creation of CoEs for metaverse in India, such as the International Hub for Education in Mixed Reality[12] by the Karnataka Digital Economy Mission, Excelsoft Technologies, Mysuru and UNESCO Mahatma Gandhi Institute of Education for Peace and Sustainable Development. At a global level, KPMG is set to establish its Centre of Excellence for Metaverse and digital twins in Saudi Arabia[13].

Policymakers may strengthen CoEs for the metaverse by promoting their creation and increasing investments in such initiatives. Regulators like the Securities and Exchange Board of India have developed an overarching framework and guidelines for how their regulatory sandboxes should function, and a similar approach may be adopted to streamline and strengthen the priorities, operations and functioning of CoEs. CoE can also be strengthened by enabling ongoing platforms for long-term dialogue and cooperation with industry stakeholders, to share knowledge and ensure a shared understanding of these technologies as they are developed. The introduction of accelerator programs within CoEs can also enable support for industry participants to build partnerships and access resources within the metaverse market. For instance, the Dubai International Financial Centre[14] (**DIFC**) launched a Metaverse Accelerator Programme to support innovative metaverse start-ups by helping them explore partnerships, gain exposure to investors, access a regulatory sandbox and obtain marketing support. Similar programs should

[9] https://pulsenews.co.kr/view.php?year=2021&no=1223734

[10] https://www.tra.org.bh/en/category/innovation-license; https://www.bna.bh/en/TRAlaunchesInnovationLicense.aspx?cms=q8FmFJgiscL2fwIzON1%2BDt9x9oPiGEpnqtOtJXgZ%2Ffo%3D

[11] https://web3sandbox.telangana.gov.in/

[12] https://www.thehindu.com/news/national/karnataka/centre-of-excellence-in-metaverse-becomes-a-reality-in-mysuru/article66226244.ece

[13] https://www.arabnews.com/node/2251326/corporate-news

[14] https://innovationhub.difc.ae/programmes/Metaverse-Accelerator-Programme

be set up in India. Further, the Singapore government (through its Personal Data Protection Commission)[15] has collaborated with organisations like Open Loop to facilitate policy prototyping, which involves testing of policy measures within a controlled environment to inform the introduction of standards and guidelines for the industry. CoEs may consider exploring such collaborations.

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 effective and significant contribution in Metaverse standardisation? Kindly provide elaborate justifications in support of your response.

RESPONSE:

The metaverse will reach its full potential only if built on a foundation of common technical standards and protocols empowering both businesses and people to seamlessly navigate and travel between multiple destinations and experiences, just like we can browse the internet today freely. The development of technical standards in specific areas is therefore crucial to a baseline level of interoperability that mirrors the kind of open internet protocols we see in place today, lowering barriers to entry and facilitating market access by small firms and developers.

While such standards may be set by government bodies and global alliances like ITU, given emerging technologies like metaverse are nascent, a global industry-wide cooperation on interoperable standards will be critical to build the metaverse which drives economic value for all participants and necessary to to bring together companies and organizations that have a shared interest to develop, define, and evolve open standards that will drive a truly interoperable metaverse.

Interoperable standards and protocols are required to be developed through a multi stakeholder collaboration at standard setting organization / standard development organizations.

- Some efforts are already being made. Groups like Metaverse Standards Forum[16] hosted by Khronos Group[17], Linux Foundation, are bringing together tech companies, hardware makers, and retailers to work on standards that will begin to solve for interoperability and portability in the govern metaverse.
- The key working groups at Metaverse Standards Forum currently include the Metaverse Standards Register Working Group, which is mapping the landscape of metaverse-related standardization activities and open standards, plus exploratory groups that are looking at 3D Asset Interoperability using USD and glTF, Digital Asset Management, Real/Virtual World Integration and Privacy, Cybersecurity & Identity
  - Universal Scene Description ("USD"), will allow 3D assets to be shared and rendered across many different immersive experiences.
  - Another standard, glTF[18], the JPEG of 3D, is a royalty-free specification for the efficient transmission and loading of 3D scenes and models by engines and applications. glTF minimizes the size of 3D assets, and the runtime processing needed to unpack and use them. glTF defines an extensible, publishing format that streamlines authoring workflows and interactive services by enabling the interoperable use of 3D content across the industry.
  - Additionally, OpenXR[19] is a royalty-free open standard from the Khronos Group, created for the development of high-performance VR applications that run on multiple platforms. OpenXR aims to simplify VR development by enabling developers to reach more platforms while reusing the same code. It offers an alternate development path that allows developers to create portable code that can be used on devices from multiple vendors.

[15] https://openloop.org/programs/ai-transparency-explainability-singapore-2/

[16] https://metaverse-standards.org/domain-groups/

[17] https://www.khronos.org/

[18] https://www.khronos.org/gltf/#:~:text=glTF%20defines%20an%20extensible%2C%20publishing,IEC%2012113%3A2022%20International%20Standard.

[19] https://www.khronos.org/openxr/

- The Linux Foundation is a nonprofit organization focused on fostering innovation through open source, has established the formation of the Open Metaverse Foundation (OMF)[20] with a mission to provide a collaboration space for diverse industries to work on developing open source software and standards for an inclusive, global, vendor-neutral and scalable Metaverse,

Given the potential of metaverse, Indian stakeholders including developers, experts, companies, startups, academia should look to actively participate and contribute to the global standard setting process. In this context, policymakers in India can consider the various measures to support, contribute and lead efforts towards the evolution of the global standard setting process.

(a) *Support international, multi-stakeholder efforts to develop baseline technical standards on an evolving basis*: India has a strong and burgeoning community of developers and open-source innovators who are well-placed to contribute to the creation of global standards, at various standard setting bodies including at the ITU. Policymakers in India should enable, encourage and support these communities and other industry participants to engage in industry-led efforts and alliances, to ensure that domestic principles are accounted for and built into these standards.

(b) *Align domestic requirements with globally agreed standards:* To enable the streamlined and cohesive growth of the domestic Metaverse industry, India policymakers must ensure that any regulation, policy measure or initiative in relation to standards accounts for corresponding international multi-stakeholder efforts, to enable alignment with global best practices. For instance, requirements in relation to Mandatory Testing and Certification of Telecom Equipment by the Department of Telecom or standards in relation to manufacture and import of products issued by the Bureau of Indian Standards should be aligned with international standards in relation to the Metaverse, to the extent applicable.

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 of a national level mechanism to coordinate development of Metaverse standards and guidelines? Kindly give your response with reasons along with global best practices.

RESPONSE

As opposed to a single governance mechanism to regulate the Metaverse, it is proposed that a multi-layer framework be adopted to meet various governance needs of the ecosystem.

(a) *Existing legal framework:* As mentioned above in Question 19, there is no separate need for a regulatory framework to govern the development and use the metaverse as the metaverse does not exist in a regulatory vacuum. The current legislative framework goes a long way in effectively governing the industry and adequately addresses issues arising out of or in connection with the metaverse. Any contemplation of a fresh legislative framework to govern the metaverse could create regulatory uncertainty, arising from overlaps with existing laws.

(b) *Policy Measures:* The government may consider policy mechanisms and incentives to drive holistic development and inclusive adoption of the metaverse. It could consider measures such as tax breaks or subsidies to encourage collaborative development of metaverse technologies. For instance, the Dubai Municipality has announced a partnership with private companies and investors to create a futuristic, human-centred city in the metaverse called 'One Human Reality'. Meanwhile, the South

[20] https://c212.net/c/link/?t=0&l=en&o=3760027-1&h=209313045&u=https%3A%2F%2Fwww.openmv.org%2F&a=Open%C2%A0Metaverse+Foundation

Korean government has announced a $186.7 million package to simulate a government led metaverse ecosystem, with a focus on encouraging young talent and fostering a culture of convergence.

(c) *Multi-stakeholder approach:* It is crucial for government, industry participants, civil society, technology experts, users and other relevant stakeholders to come together in various ways to determine how the metaverse is governed, with the aim of promoting dialogue and discussion, enabling sharing of information and best practices, and developing joint standards or guidelines for effective governance. This may be done in various ways through consultation or committees, as described above in the response to Question 17.

Q,.20 (ii). Whether there is a need of a national level mechanism to coordinate development of Metaverse standards and guidelines? Kindly give your response with reasons along with global best practices.

RESPONSE

Policymakers may consider the creation of a central multi-stakeholder agency to coordinate and build a consensus on domestic priorities and interests in relation to metaverse standards and guidelines. For instance, the Electronics and Information Technology Division council (LITDC) at the Bureau of Indian Standards[21], recently established a new panel on metaverse. The scope of the metaverse panel is as follows:

- Mirror the work of ISO/IEC SEG 15 & finalize India's inputs on their documents along with attending their meetings.
- Investigate the needs for standardization in the area of metaverse, taking into account current research, technology and standardization activities, and trends.
- Recommend an initial roadmap for standardization activities in the area of metaverse.
- Make further recommendations to LITDC as appropriate.

The endeavour of policy makers should be to support industry-led, consensus-based multi-stakeholder approaches to the development of technology standards. Please see our response to Question 17 for further details.

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?

RESPONSE

There is a compelling need to establish a regulatory framework for content moderation in the metaverse. The metaverse, as a virtual shared space where users interact with a computer-generated environment and each other, presents a unique set of challenges related to content. The diversity of cultural norms and values, coupled with the potential for harmful or illegal content such as hate speech, misinformation, cyberbullying, and child exploitation, underscores the importance of regulatory measures. Following are some reasons supporting the need for a regulatory framework.

a. Cultural Sensitivity and Diversity - The metaverse is a global platform that brings together users from diverse cultural backgrounds. A regulatory framework can help ensure that content moderation policies are sensitive to cultural differences, preventing the imposition of a one-size-fits-all approach and respecting the varied norms and values of users.

[21] https://www.services.bis.gov.in/php/BIS_2.0/bisconnect/dgdashboard/committee_sso/deptwise_panelDetails/66

b. Protection Against Harmful Content - Establishing regulations is crucial for protecting users from harmful content, including hate speech, misinformation, cyberbullying, and child exploitation. A framework can provide guidelines for identifying and addressing such content, creating a safer virtual environment for users.

c. Legal Compliance - a regulatory framework ensures that content moderation practices align with existing legal frameworks. This is essential for holding platforms accountable and providing a basis for legal action in cases of non-compliance with content standards or in the presence of illegal content.

d. User Privacy and Data Protection - regulations can address concerns related to user privacy and data protection in the metaverse. Clear guidelines can help platforms establish transparent data practices and ensure that user information is handled responsibly and ethically.

e. Age-Appropriate Content - given the potential for child exploitation, a regulatory framework can establish guidelines for age-appropriate content. This includes mechanisms for verifying user ages and implementing measures to protect minors from exposure to inappropriate material.

f. Stakeholder Collaboration - regulations encourage collaboration between platform providers, content creators, and regulatory bodies. Working together, these stakeholders can develop effective content moderation strategies that balance creativity, freedom of expression, and the need for a safe and respectful online environment.

g. Public Accountability - Establishing a regulatory framework enhances public accountability for metaverse platforms. Users and the broader public can have confidence that there are clear standards in place, and platforms can be held accountable for their content moderation practices.

In addition to the above, the issue of deepfakes posing significant challenges and concerns in India. Deepfakes are AI-generated content, often involving manipulated audio, video, or images, which can convincingly depict individuals saying or doing things they never did. In India, this technology raises several specific problems.

As per the Hon'ble Minister of Communication statement given to the media – India is going frame new regulation over deepfake within 10 days.

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?
ii. What are the main challenges and gaps in content moderation in the Metaverse?
iii. What are the best practices and examples of effective content moderation in the Metaverse or other similar spaces?
iv. What are the key principles and values that should guide content moderation in the Metaverse?
v. How can stakeholders collaborate and coordinate on content moderation in the Metaverse?

RESPONSE:

In light of the new Telecom Bill -2023, passed by both the houses of the parliament very recently, it will be

appropriate to review the comments and necessary changes if any, may be incorporated.
Various laws already exist on content moderation, which will equally apply to content in the metaverse. Consequently, there is no need for the development of a regulatory framework to specifically govern content moderation in the metaverse. We have briefly set out some of these laws below.

(a) *Information Technology and Intermediary Laws:* The (Indian) Information Technology Act, 2000 read with the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (**Intermediary Rules**) prescribes content related due-diligence requirements for intermediaries and requires them to inform the user to not host, display, upload, modify, publish, transmit, store, update or share a variety of information that may be harmful including information that belongs to another person, is obscene, pornographic, paedophilic, invasive of another's privacy, is insulting or offensive, is harmful to child, deceives or misleads the reader, threatens national security, contains any harmful code or virus, or is otherwise violative of any laws in force. Intermediaries are required to remove or disable access to any such information voluntarily, on the basis of grievances received, or if they receive official communication from the government or court. Given the active enforcement of this law, it can be effectively used to govern content in the Metaverse.

The proposed Digital India Act, which looks to revamp the existing legal framework for information technology, also places a considerable emphasis on content moderation. It looks to introduce regulation to protect users of digital spaces, including measures to prevent cyber-bullying, misinformation, and regulate content targeting children.

(b) *Criminal Laws:* The IPC prescribe penalties for *inter alia* the distribution, public exhibition or circulation of 'obscene' material and the participation in a business in the course of which one knows/has knowledge to believe that obscene material may be conveyed. Case law suggests that this may include material like video clips of sexual acts involving minors, or content which is *per se* inflammatory, unacceptable by community standards, or is demeaning, degrading and obscene. These provisions are therefore likely to cover a range of content and user behaviour that may be harmful in the Metaverse. The IPC also prescribes penalties for defamation and harm to reputation. As mentioned above, interests of women and children in relation to content on the metaverse are also protected through the POCSO and the Indecent Representation of Women (Prohibition) Act, 1986. Separately, the Constitution of India provides individuals with the fundamental right to privacy and the right against discrimination, while tort law provides sufficient legal recourse to individuals in instances where their personal information or proprietary information is misused or create 'obscene' material. Information technology laws also prescribe criminal penalties for the publishing or transmission of any sexually explicit content, particularly those relating to children.

Therefore, restrictions under existing laws allow for considerable content moderation in connection with any content displayed or transmitted in the metaverse or services availed in the metaverse.

In addition to legislation, there exist various self-regulatory codes and guidelines that also serve to regulate content and ensure user safety. For example, Advertising Standards Council of India (**ASCI**) is an industry organization, which has issued a voluntary Code for Self-Regulation (**ASCI Code**) to advertisers that acts as a model of conduct in connection with advertisements. The Guidelines for Prevention of Misleading Advertisements and Endorsements for Misleading Advertisements, 2022 (**Misleading Ads Guidelines**) also contain conditions for a valid advertisement and advertisements targeted at specific sets of individuals such as children and is applicable to all advertisements regardless of form, format or medium. Any advertising content in the metaverse would fall within the purview of these codes.

The Intermediary Rules contemplates a three-tier regulatory framework for grievance redressal (including grievances related to content in the metaverse), primarily comprising self-regulatory bodies. A Code of Ethics under these rules also indicates guidelines in relation to restricting certain content in the case of children and classifying content for various age-grounds based on its nature. Separately, most metaverse platforms are likely to implement internal community guidelines as well as robust top-down content moderation systems to keep a close watch on the content hosted and transmitted by these platforms.

Further, in order to assess the application of these existing laws to the metaverse and analyse new risks that may arise in relation to content moderation, a multi-stakeholder approach to assess the need for regulation or intervention may be adopted, as described further in our response to Question 17.

Q.23. 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.

RESPONSE:

The existing legal framework in India for intellectual property rights (**IPR**) is adequately robust to protect and enforce IPRs in the metaverse. The Indian Copyright Act, 1957 penalises the act of knowingly infringing or abetting infringement of copyright or any other right granted under the Copyright Act. Similarly, under the Trademarks Act, 1999, the registered proprietor of the trademark is entitled to certain exclusive rights in relation to the use of the trademark for the goods and services it was registered for. Further, the Patents Act, 1970 grants an exclusive right to a patentee to prevent third parties from using the patented product or process without any authorisation. These protections would equally extend to the IPR involved in activities within the metaverse or for the development of metaverse. We have briefly addressed the adequacy of these laws below.

(a) *Identifying and registering IPR in the metaverse:* Existing laws enable each metaverse user to make relevant submissions and proceed under the prescribed current registration process associated with the category of IP that they are looking to protect. Reports indicate that 'metaverse-related' trademark registration filings are on the rise with several filings in registers in the US[22], EU[23] and the Indian Trademark Registry[24]. Similarly, several leading players in the market such as Meta, Sony, Xiaomi, Microsoft have made patent filings and secured registrations for metaverse-related technologies such as VR, chips, and operating systems across the globe. The volume of such filings in global registers indicate that the existing IP registration framework enables registration and effective protection of 'metaverse-related' IPR.

(b) *Protecting and Enforcing IPRs in the metaverse:* Enforcement of IPRs may look different in the metaverse and may require additional measures to be taken. While these measures continue to operate within the existing framework of IPR in India, they may require additional resources, capacity-building and training of personnel.

    For example:

    - Monitoring IPR infringement on metaverse platforms can be done using tools made available by market players or by relying on the services of specialised service providers in this regard. metaverse platforms would also be required to undertake reasonable efforts to monitor IPR

[22] https://www.forbesindia.com/article/crypto-made-easy/data-claims-that-trademark-application-for-crypto-nfts-and-metaverse-projects-increase-in-2022/79611/1
[23] https://europeanbusinessmagazine.com/business/nft-and-metaverse-trademark-filings-more-than-double-in-2022-despite-crypto-winter/
[24] https://spicyip.com/2022/05/trademarks-and-the-metaverse-imaginary-rights-or-real-wrongs.html

infringing content on its platforms as part of its due-diligence requirements under the Intermediary Rules as discussed in our response to Question 22.

- Enforcing IPR may continue using traditional means of enforcement such as injunctions, cease and desist letters, seizure of digital assets and notice and take down procedures. However, intellectual property authorities may increasingly require the support of metaverse platforms to be able to access the virtual world in order to enforce IPR claims.
- Criminal investigations of IPR crime may need to be modified, with cyber patrol, content moderation, and dedicated task forces for the metaverse.

Given that metaverse development is in its nascent stages of development, we recognise that there may be concerns that arise in relation to the registration and protection of IPR. Efforts to regulate IPR in the metaverse should not be done domestically in a silo, given the need for interoperability across virtual environments. This is in line with the global approach, given that jurisdictions across the globe are currently assessing the adequacy of existing IPR laws to the metaverse. In this regard, various international organisations have opened dialogues to consider emerging issues in IPR in the metaverse. For instance, the Observatory on infringement of IPR entrusted to the EU IPO has commenced a workstream on the impact of the metaverse on infringement and enforcement of IPR. Given that IPR rights are currently domestically governed, instruments like international multilateral treaties may be critical in ensuring the enforcement of a cohesive global agreement on IPR protection in the metaverse. India should lead and participate in global conversations and agreements around protection and enforcement of IPR in the metaverse, in order to ensure that domestic needs are addressed, and to ensure adoption of global best practices in this regard.

Q.24. Please comment on any other related issue in promotion of the development, deployment and adoption of 5G use cases, 5G enabled IoT use cases and Metaverse use cases in India.
Please support your answer with suitable examples and best practices in India and abroad in this regard.

RESPONSE:

The existing legal framework in India for intellectual property rights (**IPR**) is adequately robust to protect and enforce IPRs in the metaverse. The Indian Copyright Act, 1957 penalises the act of knowingly infringing or abetting infringement of copyright or any other right granted under the Copyright Act. Similarly, under the Trademarks Act, 1999, the registered proprietor of the trademark is entitled to certain exclusive rights in relation to the use of the trademark for the goods and services it was registered for. Further, the Patents Act, 1970 grants an exclusive right to a patentee to prevent third parties from using the patented product or process without any authorisation. These protections would equally extend to the IPR involved in activities within the metaverse or for the development of metaverse. We have briefly addressed the adequacy of these laws below.

(c) *Identifying and registering IPR in the metaverse:* Existing laws enable each metaverse user to make relevant submissions and proceed under the prescribed current registration process associated with the category of IP that they are looking to protect. Reports indicate that 'metaverse-related' trademark registration filings are on the rise with several filings in registers in the US[25], EU[26] and the Indian Trademark Registry[27]. Similarly, several leading players in the market such as Meta, Sony, Xiaomi, Microsoft have made patent filings and secured registrations for metaverse-related technologies such as VR, chips, and operating systems across the globe. The volume of such filings in global registers

[25] https://www.forbesindia.com/article/crypto-made-easy/data-claims-that-trademark-application-for-crypto-nfts-and-metaverse-projects-increase-in-2022/79611/1
[26] https://europeanbusinessmagazine.com/business/nft-and-metaverse-trademark-filings-more-than-double-in-2022-despite-crypto-winter/
[27] https://spicyip.com/2022/05/trademarks-and-the-metaverse-imaginary-rights-or-real-wrongs.html

indicate that the existing IP registration framework enables registration and effective protection of 'metaverse-related' IPR.

(d) *Protecting and Enforcing IPRs in the metaverse:* Enforcement of IPRs may look different in the metaverse and may require additional measures to be taken. While these measures continue to operate within the existing framework of IPR in India, they may require additional resources, capacity-building and training of personnel.

For example:

- Monitoring IPR infringement on metaverse platforms can be done using tools made available by market players or by relying on the services of specialised service providers in this regard. metaverse platforms would also be required to undertake reasonable efforts to monitor IPR infringing content on its platforms as part of its due-diligence requirements under the Intermediary Rules as discussed in our response to Question 22.
- Enforcing IPR may continue using traditional means of enforcement such as injunctions, cease and desist letters, seizure of digital assets and notice and take down procedures. However, intellectual property authorities may increasingly require the support of metaverse platforms to be able to access the virtual world in order to enforce IPR claims.
- Criminal investigations of IPR crime may need to be modified, with cyber patrol, content moderation, and dedicated task forces for the metaverse.

Given that metaverse development is in its nascent stages of development, we recognise that there may be concerns that arise in relation to the registration and protection of IPR. Efforts to regulate IPR in the metaverse should not be done domestically in a silo, given the need for interoperability across virtual environments. This is in line with the global approach, given that jurisdictions across the globe are currently assessing the adequacy of existing IPR laws to the metaverse. In this regard, various international organisations have opened dialogues to consider emerging issues in IPR in the metaverse. For instance, the Observatory on infringement of IPR entrusted to the EU IPO has commenced a workstream on the impact of the metaverse on infringement and enforcement of IPR. Given that IPR rights are currently domestically governed, instruments like international multilateral treaties may be critical in ensuring the enforcement of a cohesive global agreement on IPR protection in the metaverse. India should lead and participate in global conversations and agreements around protection and enforcement of IPR in the metaverse, in order to ensure that domestic needs are addressed, and to ensure adoption of global best practices in this regard.