Nasscom's Feedback on Telecom Regulatory Authority of India Consultation Paper on Digital Transformation through 5G Ecosystem

Ms. Vandana Sethi
Advisor (Admin)
Telecom Regulatory Authority of India

December 26, 2023

SUMMARY OF RECOMMENDATIONS

REGULATORY CONSIDERATIONS FOR 5G & IoT

Recommendation 1

- *The government should ensure that Indian Industry has sufficient representative participation in global standard making bodies.*
- *Through public private partnership we should develop and implement 5G use cases.*
- *Involvement of local government bodies, schools and other community organizations, and relevant government agencies to spread awareness of 5G and its use-cases.*
- *Prepare in consultation with the industry a roadmap for a sunset date for 2G and 3G networks to give greater impetus to developing ecosystem to 5G use cases.*
- *There is a further need to smoothen the approval processes and reduce the fees with regards to ROW, permissions for use of street furniture for small cell and aerial fibre deployment etc. We will be pleased to work with the industry and the TRAI to identify specific details.*
- *EMF radiation norms should be aligned with ICINRP limits to improve the quality of services.*

Recommendation 2

We have not received feedback from the industry on 5G enabled IoT use cases in India. Currently IoT devices operate on 4G. The 4G network is comparatively slower than 5G but it covers larger distances, when 5G roll-out improves, IoT devices may switch to 5G. The use cases may become more apparent then.

We have received input from the industry in the context of M2M. To the extent that IoT is seen as an evolution from and a subset of M2M, the inputs may be considered. For detailed input, please refer to page no 9 & 10 of our feedback.

Recommendation 3

Under the present framework, IoT device hardware is to be tested as per ER prepared by TEC, and the software by STQC. Therefore, there is no need for additional measures for strengthening the NTC framework.

Recommendation 4

Effectiveness of the DPDP Act in addressing IoT-related concerns will depend on delegated legislation and the operational practices initiated by the Data Protection Board, which is yet to be released. Therefore, any evaluation with respect to whether the DPDP Act adequately covers and mitigates issues pertinent to IoT device security must be done at a later stage once such delegated legislations have come into force and the jurisprudence on privacy law in India has developed.

Recommendation 5

- *Any risks pertaining to IoT first be measured against the existing regulatory measures and frameworks.*
- *Any additional risks not already covered may be explored on a case-to-case basis through a multi-stakeholder approach. This will avoid overlapping and excessively onerous regulatory frameworks, which may result in stifling innovation.*
- *Further, establishing voluntary industry-specific standards and guidelines outlining best practices will ensure a more uniform and consistent approach in handling liability concerns.*

REGULATORY CONSIDERATIONS FOR METAVERSE

Recommendation 6

- *For awareness: Using public private partnership, awareness campaigns and exhibitions should be funded and organised, to demonstrate best practices within the industry and to make the public aware of new and existing use cases.*

- *For access: make available high speed internet connectivity at affordable rates. Accessibility also means providing opportunities and solutions for people with disabilities. Public private partnership can be explored to integrate metaverse into existing systems, like provide remote skilling, promote rural tourism, provide citizen services, build community centres equipped with high-speed internet and metaverse supporting hardware like AR/VR headsets, etc.*

- *For skilling: Present educational curriculum (both at school and college level) can be updated to meet the needs of emerging technologies like AR, VR, MR, and AI. This could include introducing internship and skill-development programmes at the school and college level.*

Recommendation 7

- *Based on the feedback received from industry, we have not found gaps or specific concerns in the existing laws with respect to regulation of the metaverse. There are existing laws, like, information technology, cybersecurity, consumer protection and payment laws along with self-regulatory codes which are applicable to metaverse. Therefore, at this juncture, when the metaverse is in the early stages of development, the regulatory focus should ideally be on reviewing the applicability and effectiveness of existing and upcoming legislations in the metaverse context.*

- *We have listed below some of the applicable existing laws, Code, guidelines, and order that will apply to issues emerging in the metaverse:*

  - *Digital Personal Data Protection Act, 2023*

  - *Information technology and cybersecurity law [Information Technology Act, 2000]*
  - *Criminal laws [Protection of Children from Sexual Offences Act, 2012, and Indian Penal Code, 1860]*
  - *Consumer protection law [Consumer Protection Act, 2019]*
  - *RBI regulations, directions, schemes, and notifications*
  - *Self-regulatory codes [soft law guidance – Guidelines for Prevention of Misleading Advertisements and Endorsements for Misleading Advertisements, 2022, The Code for Self-Regulation of Advertising Content in India]*
  - *Mandatory Testing and Certification of Telecom Equipment regime Electronics, and Information Technology Goods (Requirements for Compulsory Registration) Order, 2021*

- *Further, the proposed Digital India Act is likely to play a key role in addressing these risks and considerations in regulating the Indian technology landscape. Should there be any gaps between current regulations and challenges emerging in the metaverse, the government can consider addressing them in the proposed law.*

Recommendation 8

- *The ecosystem of regulatory sandboxes (like, experimental campus) should be encouraged, and multiple sandboxes must be set up to assess potential risks and benefits of a new technology, while allowing industry participants the flexibility to reiterate as required.*
- *Accelerator programs should be introduced within the Centre of Excellences for industry participants to build partnerships and access resources within the metaverse market.*

Recommendation 9

- *Requirements in relation to the Mandatory Testing and Certification of Telecom Equipment by the Department of Telecommunications 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.*

- *The government, industry participants, civil society, technology experts, users, and other relevant stakeholders should collaborate in various ways to determine how the metaverse is governed, for enabling sharing of information and best practices, and developing joint standards or guidelines for effective governance.*

Recommendation 10

The government must undertake a more proactive approach through greater participation (including industry) in these standard-setting processes to ensure that India plays an important role in the formulation of international governance rules and standards.

Recommendation 11

- *We have not received feedback from stakeholders highlighting any specific concern or challenge in terms of registration of IPR in metaverse or enforcement/protection of IPR in the metaverse, interoperability and compatibility of IPRs across different virtual environments which may require modification to the existing IPR framework. Hence, we cannot recommend any modification to the existing IPR framework.*

- *When any such specific IPR challenge or risk arises and brought to our notice, questions like, whether the concerned issue is related to the Trademarks Act, Copyright Act or Patents Act; what exactly the nature of concern is, which provision of the given law needs to be analysed, whether it can be addressed through issuance of guidance/FAQs or through parliamentary intervention, could be examined on a case-to-case basis.*

- *We recommend that India should participate in global conversations and multi-stakeholder's approach in various IPR issues around metaverse including interoperability and compatibility of IPRs across different virtual environments.*

Recommendation 12

We have received feedback from industry that the government may consider delicensing 6Ghz for wider economic benefits, including to spur the growth of metaverse ecosystem. Our recommendation aligns with scenario 2 – unlicensed, as one of the regulatory options suggested by the TRAI in its white paper on 6 GHz band. In case there are specific concerns with delicensing these should be separately discussed, and a decision taken in the overall economic interest.

INTRODUCTION

Nasscom welcomes the opportunity to provide feedback on the Consultation Paper on *Digital Transformation through 5G Ecosystem,* issued by the Telecom Regulatory Authority of India (**TRAI**) on 29 September 2023 (**CP/5G CP/Consultation Paper**).[i]

The 5G CP seeks to identify the policy challenges and suggest the right framework for faster adoption and effective utilisation of new technologies [such as Internet of Things (**IoT**), metaverse, Augmented Reality, Virtual Reality (**AR/VR**)], in order to fully realise the potential of 5G technology. To this extent, it puts forth various questions pertaining to regulatory measures required for the development of such new technologies.

Our feedback address two broad themes – (i) regulatory considerations for 5G & IoT; and (ii) regulatory considerations for the metaverse, including content moderation and regulation of intellectual property in the metaverse.

We have responded to selected questions (**2, 3, 5, 9, 10, 11, 14, 16-24**) of the Consultation Paper. For the remaining questions, we have not received feedback from the industry.

However, before we proceed to provide question-wise response, following are our general observations on the CP:

1. ***Design a focused scope for consultation***: The CP is highly informative and provides useful updates especially on global developments in the field of emerging technologies. But as a CP, it attempts to cover too many issues, and some of these may not even fall within the jurisdiction of the TRAI. For instance, the CP attempts to cover IoT ecosystem in the context of privacy and cybersecurity concerns; skilling for Industry 4.0; challenges faced by MSMEs in adoption of Industry 4.0; privacy, cybersecurity, and content moderation in metaverse; IPR protection in metaverse; standardisation in metaverse; use of open government data, monetisation and sharing of data; and many more.

   Attempting to cover multiple complex themes in one CP could impact the depth of discussion and feedback. **We request the TRAI to confine the coverage of future consultation papers to a group of selected high priority themes/agenda items so the engagement with stakeholders is more focused and meaningful.**

2. ***Provide clear evidence-based problem statement***: Some of the questions raised in the CP are **not evidenced by a clear problem statement** in the Indian context, nor does it point out to any existing specific gaps in the regulatory framework, like any particular provision in the law, rules, or regulations. Highlighting these specific points (like any specific recent development, consumer complaint, market trend, clear reasons making a case why the existing framework may be falling short) can help us to engage with industry in a more focused manner and possibly give specific feedback.

   For instance, in the **section on metaverse**, the CP states: *the rise in virtual interactions and the unique features of the metaverse means greater sharing of data. This may lead to a surge in threats of data breaches and concerns around how technology companies collect*

> *and process the personal data of people. These concerns are all the more prominent for countries like India that still do not have a dedicated data protection legislation.* (**Para 4.65**).
>
> *In addition to data theft concerns, the increase in virtual interactions and the growth of concepts like digital avatars will make the tracking of cybercriminals and interception of illegal content more pernicious. The questions of legislations and jurisdictions that will be applicable in this boundless digital world is also a prominent concern requiring consideration by lawmakers.* (**Para 4.66**)

Immediately after the above paragraphs, it raises the question – *whether there is a need to develop a regulatory framework for the responsible development and use of metaverse and if yes, how that framework is going to address concerns like users controlling their personal information, data privacy and security in metaverse, etc,* (**Q no 17**).

While some of these concerns are legitimate and needs consideration, it is not clear the rationale behind the question on need for a regulatory framework, given merely few months back India legislated its first data protection law.

Also, the CP while discussing these concerns, does not make out a clear case pointing out that the existing laws could be inadequate or ill-equipped to address them. In addition to the DPDPA, the government is contemplating to replace the Information Technology Act with the Digital India Act which aims to address several users' safety concerns around the emerging technology. Interestingly, the CP acknowledges the recent legislation of the DPDPA, but strangely in some sections, it does not find a mention (**see the above underlined sentence of Para 4.65**).

Similarly, the **question on IoT** states: "*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*". (**Question no 11**)

This question comes immediately after the paragraphs which refers to various sections of the IT Act, DPDPA and TRAI's Recommendation on "Privacy, Security and Ownership of Data in the Telecom Sector". Further, it is not clear whether the question is referring to the scope of rules/delegated legislation under the DPDPA or any other/new regulatory intervention.

Again, the **section on IPR** (**Para 4.78 to 4.80**) of the CP seeks suggestions on *modification in the existing legal framework in a broad stroke citing issues like identification and registering IPRs in the metaverse, protection of IPR, interoperability across different virtual environments* (**Q no 23**).

However, the discussion does not spell out for instance, what is the nature of IPR challenge with respect to registration of IPR, so it could be examined on a case-to-case basis. For instance, in para 4.79 of the CP states *that – "Another issue is the jurisdictional complexity and uncertainty of the metaverse. The metaverse is not bound by physical borders or national laws, but rather by the rules and policies of different platforms and service providers."*

While this is true but similar jurisdictional concerns have existed in the context of online platforms where IPR infringement issue has arisen beyond the territorial jurisdiction. At least from the information provided in the CP, it is not very clear how the jurisdictional issue is unique to the case of metaverse.

Immediately in the next **para 4.80,** the CP states that "*the existing legal framework may not be adequate to address the IPR issues in the metaverse, such as infringement, ownership, licensing, and enforcement. Therefore, some modifications are required in the legal framework to address these issues.*"

On the contrary, reports indicate that 'metaverse-related' trademark registration filings are on the rise with several filings in registers in the US, EU and the Indian Trademark Registry (application filed for registration of trademarks in relation to 'downloadable virtual goods' and online virtual services).[ii] Similarly, some of the global players in the metaverse market have made patent filings and secured registrations for metaverse-related technologies such as VR, chips, and operating systems.

Further, the CP does not specify whether the concerned issue is related to the Trademarks Act, Copyright Act or Patents Act and within each legislation, what exactly is the nature of concern that has come to the notice of TRAI. Only once the problem statement is clearly defined, it can be examined meaningfully to ascertain whether any modification to the existing framework is required or not.

3. ***Balance innovation and regulatory obligations***: Finally, we submit that development of IOTs and metaverse is still in a nascent stage in India. Our thinking around regulatory approach should focus not only address concerns but also serve as a catalyst for growth, propelling India to the forefront of metaverse development and innovation.

RESPONSE TO REGULATORY CONSIDERATIONS FOR 5G & IoT

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.:

RESPONSE:

The regulatory framework should become conducive for massive 5G deployment by supportive framework for EMF by adoption of ICNIRP norms for EMF. Recently, the government in response to a Parliamentary question (dated August 11, 2023) has submitted that exposure limit recommended by the ICNIRP norms (recommended by both WHO and ITU) do not produce any known adverse health. The government in the same parliamentary response has stated that it has adopted extremely strict norms for EMF radiation which is 10 times more stringent than the safe limits prescribed by ICNIRP.

However, the Parliamentary response does not clarify the reason for adoption of such stricter norms. As per inputs from the industry, such stricter EMF radiation norms severely impacts the quality of services.

We have received feedback from the industry that there is a further need to smoothen the approval processes and reduce the fees with regards to ROW, permissions for use of street furniture for small cell and aerial fibre deployment etc. **We will be pleased to work with the industry and the TRAI to identify specific details.**

Another step to consider would be to agree on a roadmap for a sunset date for 2G and 3G networks completely so that unnecessary network costs should be avoided, and all customers can be migrated to 4G and 5G services. This will also give greater impetus to developing ecosystem to 5G use cases. **This roadmap should be prepared in consultation with the industry.**

We have received suggestion from the industry that cross-sectoral collaboration can be enhanced by providing open, independent, and non-obtrusive platform that brings together all the interested parties i.e. TSPs, generational transformation professionals from industries like, healthcare, manufacturing and education, and all other relevant areas on one platform. **This suggestion may be explored in detail by the TRAI for it to be evaluated.**

The government should ensure that Indian Industry has sufficient representative participation in global standard making bodies. This will help ensure that our emerging use cases conform with the evolving global common standards for 5G applications across sectors. This in turn will facilitate interoperability and seamless integration.

Government should encourage the public sector enterprises and Government departments to collaborate with private companies on equal footing to develop and implement 5G use cases.

While there is awareness of 5G in urban areas and many of the rural areas, we may need to create awareness of 5G and its use cases in many rural areas. This can be addressed through effective communication strategies with the involvement of local government bodies, schools and other community organizations, banks, agricultural cooperatives, and relevant government agencies.

Recommendation 1

- *The government should ensure that Indian Industry has sufficient representative participation in global standard making bodies.*
- *Government in partnership with the private sector should develop and implement 5G use cases.*
- *Involvement of local government bodies, schools and other community organizations, and relevant government agencies to spread awareness of 5G and its use-cases.*
- *Prepare in consultation with the industry a roadmap for a sunset date for 2G and 3G networks to give greater impetus to developing ecosystem to 5G use cases.*
- *There is a further need to smoothen the approval processes and reduce the fees with regards to ROW, permissions for use of street furniture for small cell and aerial fibre deployment etc. We will be pleased to work with the industry and the TRAI to identify specific details.*
- *EMF radiation norms should be aligned with ICINRP limits to improve the quality of services.*

Q.3. 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?

RESPONSE:

We have not received feedback from the industry on 5G enabled IoT use cases in India. Currently IoT devices operate on 4G. The 4G network is comparatively slower than 5G but it covers larger distances, when 5G roll-out improves, IoT devices may switch to 5G. The use cases may become more apparent then.

There are many regulatory hurdles that hinder the growth of use of IoT or M2M communication, it is critical to address these issues to help proliferation of IoT services in rural areas.

Recommendation 2

We have received input from industry in the context of machine 2 machine (M2M) communication. **To the extent that IoT is seen as an evolution from and a subset of M2M, the following inputs may be considered.**

(i) The M2M communication related instructions dated 30.05.2019, mandate that data communication for M2M SIMs can be allowed only to 4 predefined public URLs/ IPs. This restriction is not in consonance with market realities. This restriction is proving to be a major issue with the most popular M2M solutions. This restriction is also against the international precedents in countries making rapid advances in M2M communications like the U.S.

As the M2M solutions are a result of collaborative efforts between multiple entities handling different legs of the M2M solution, restriction of 4 IPs effectively constrains the innovations and effective M2M solutions and needs to be removed.

Standardisation/certification of IoT/M2M device

(ii) There is a need for uniform policy based on GSMA standards for integration of Subscription Manager Secure Routing (SM-SR) platform for all the M2M devices being imported in the country. One approach can be to ensure that while SM-DP remains within India, the SM-SR is allowed across the geographical boundaries to cater various use case requirements.

(iii) e-SIM personalisation or remote provisioning should be carried out through the systems and facilities duly certified by SAS of GSMA. The SM-DP, SM-DP+ used for e-UICC personalisation should be located within the geographical boundaries of India. The SM-SR, SM-DS and remote OTA platform should also be preferably hosted in India.

(iv) As IoT/M2M applications cover critical areas such as manufacturing, telemedicine & healthcare, connected vehicles, home equipment, smart meters etc., these should not be covered under the data services shut down orders issued by the government authorities.

(v) The enterprise and non-P2P usage character with restricted communication abilities of M2M SIMs should lead to exemption from tele-verification requirements, that are essentially for bona-fide personal use are not relevant in this scenario.

(vi) We submit that with the advances in technology, eSIM is becoming increasingly popular with much adaptation in M2M devices. TRAI should facilitate easy import of eSIM produced outside, a measure that will also facilitate import of vehicles /devices from global manufacturers.

(vii) The integrated SIM (**ISIM**) technology is cost-effective and a boon for low power M2M devices that have multiple usage, especially in remote areas and should be permitted with suitable security safeguards as per 3GPP and GSMA guidelines.

(viii) For M2M applications, there are many default URLs, DNS, Device Management URLs, firmware upgrade, remote SIM management etc., connectivity to which is imperative for effective services. There should be no restriction on connectivity with these URLs and it should be made available on default basis as these URLs will not carry any customer or application specific data but will only help in delivering better services and management.

(ix) Many of the M2M devices are deployed for various purposes such as street lighting, smart parking etc. where end custodian cannot be assigned, thus it should not be mandatory to provide the same periodically.

Q.5. 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 justifications in line with the global best practices.

RESPONSE:

Testing and Certification of IoT devices hardware is already covered in Essential Requirements (**ERs**) under the Mandatory Testing and Certification of Telecommunication Equipment (**MTCTE**) with testing specifications related to electromagnetic compatibility, safety, communication interfaces, specific absorption rate (**SAR**), and security. Thus, under the present framework, IoT device hardware is to be tested as per ER prepared by TEC, and the software by Standardisation Testing and Quality Certification Directorate (**STQC**). Therefore, we do not see any need for additional measures for strengthening the NTC framework.

Recommendation 3

Under the present framework, IoT device hardware is to be tested as per ER prepared by TEC, and the software by STQC. Therefore, there is no need for additional measures for strengthening the NTC framework.

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?

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?

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.

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.

RESPONSE TO Q No 9, 10, 11 & 14:

There are several existing laws that apply in the context of issues highlighted by the TRAI relating to the development or use of IoT devices. For instance, the recent enactment of the Digital Personal Data Protection Act, 2023 (**DPDP Act**) aims to provide protection of personal data of individuals, resulting in users having greater control and autonomy over their data. The DPDP Act already leverages some of the global best practices such as notice, choice, and consent mechanisms (which have also been recommended by TRAI) with respect to privacy. Such mechanisms empower users by informing them about data collection practices and granting them control over their data.

Recommendation 4

*Effectiveness of the DPDP Act in addressing IoT-related concerns will depend on delegated legislation and the operational practices initiated by the Data Protection Board (**DPB**), which is yet to be released. Therefore, any evaluation with respect to whether the DPDP Act adequately covers and mitigates issues pertinent to IoT device security must be done at a later stage once such delegated legislations have come into force and the jurisprudence on privacy law in India has developed.*

In relation to security, several frameworks in India including telecommunication laws already impose obligations on devices in relation to mandatory testing, certification, and standards, prior to sale, import or use in India. Further, existing frameworks such as the "***Code of Practice for Securing Consumer IoT***," released by Telecommunication Engineering centre, a wing of the Department of Telecommunications (**DoT**)[iii] are already in place, which specifically lay down guidelines for IoT devices and set out best practices, protocols, and standards to enhance the security and resilience of IoT devices.

Voluntary industry specific industry standards must be explored. For instance, the Cyber Security Agency of Singapore (**CSA**) has launched a voluntary cyber security labelling scheme for consumer smart devices, aiming to enhance IoT security, improve overall cyber hygiene, and enable consumers to identify products with better cyber security provisions and is based on the ETSI Standard EN 303 645.

The DoT has also issued advisory guidelines to **M2M**/IoT stakeholders for securing consumer IoT.[iv] Moreover, the DPDP Act also requires entities processing personal data to **implement technical and organisational measures** to prevent personal data breaches.

Recommendation 5

- *Any risks pertaining to IoT first be measured against the existing regulatory measures and frameworks. Any additional risks not already covered may be explored on a case-to-case basis through a multi-stakeholder approach. This will avoid overlapping and excessively onerous regulatory frameworks, which may result in stifling innovation.*

- *Further, establishing voluntary industry-specific standards and guidelines outlining best practices will ensure a more uniform and consistent approach in handling liability concerns.*

RESPONSE TO REGULATORY CONSIDERATIONS FOR METAVERSE

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:

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 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.

To make metaverse accessible to masses, we need to provide high speed internet at affordable rates. Further, accessibility doesn't just mean access to the technology. It also means providing opportunities and solutions for people with disabilities.

Further to ensure access, metaverse needs to be **integrated with the existing system**. Using 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 could be:

- remote skilling
- branding rural destinations for tourists
- providing citizen services

setting up community centres equipped with high-speed internet and metaverse supporting hardware like AR/VR headsets. These centres can serve as hubs for digital literacy training, metaverse awareness programs, and skill development workshops.

Skilling for the metaverse: Increasing innovation in the metaverse must be accompanied by upskilling of the workforce to participate in the growth of the industry. There exist significant opportunities for employment, given the advent of new job profiles such as metaverse architects, virtual event planners, AR/VR Software Engineers, and more. Present educational curriculum (both at school and college level) can be updated to meet the needs of emerging technologies like AR, VR, MR, and AI. This could include introducing internship and skill-development programmes at the school and college level. Companies have already begun investing in programs to skill students and educators in new technologies.

Integration with existing 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 could be:

- remote skilling
- branding rural destinations for tourists
- providing citizen services
- setting up community centres equipped with high-speed internet and metaverse supporting hardware like AR/VR headsets. These centres can serve as hubs for digital literacy training, metaverse awareness programs, and skill development workshops.

Recommendation 6

For awareness: Using public private partnership, awareness campaigns and exhibitions should be funded and organised, to demonstrate best practices within the industry and to make the public aware of new and existing use cases.

For access: make available high speed internet connectivity at affordable rates. Accessibility also means providing opportunities and solutions for people with disabilities. Public private partnership can be explored to integrate metaverse into existing systems, like provide remote skilling, promote rural tourism, provide citizen services, build community centres equipped with high-speed internet and metaverse supporting hardware like AR/VR headsets, etc.

For skilling: Present educational curriculum (both at school and college level) can be updated to meet the needs of emerging technologies like AR, VR, MR, and AI. This could include introducing internship and skill-development programmes at the school and college level.

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:

We have given a consolidated response to the above question through the following indicative list of existing laws, regulations, standards, and guidelines that govern the development and use of metaverse.

(i) ***Users Control over personal information and identity***: The DPDP Act 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, data minimisation can ensure that online environments do not automatically become risky environments by excessive collection and sharing indiscriminate amounts of data.

(ii) ***User Safety & security***: 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.

For instance, harassment and abuse by avatars of users in the metaverse may be addressed under existing legislations, as actions of avatars may potentially be attributed to the natural person controlling the avatar, thereby attracting penalties under the IPC and the Information Technology (**IT**) Act, 2000 for offences such as online sexual harassment and stalking.[v]

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 through rules, such measures may involve implementing data retention standard operating procedures, a notice and consent logging mechanism, encryption etc.

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.

Child users' safety will also be ensured under existing frameworks, such as the Protection of Children from Sexual Offences (**POCSO**) Act, 2012 and the IT Act, which penalise use of children in pornographic material and electronic material of such nature 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.

The 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. Such provisions under law would ensure users in the metaverse are protected against any deficient digital services and any technical issues with digital assets.

For **safety of devices**, there are existing regulatory frameworks. For instance, certificatory frameworks such as the **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.

For **payments** within the metaverse, the blockchain-enabled tools (like, **cryptocurrency**) might support digital payment processes. For instance, the present payment mechanisms involving digital fiat currency can enable purchase of digital assets and serve the metaverse ecosystem. Hence, several regulations, directions, schemes, and notifications implemented by the Reserve Bank of India (**RBI**) offer recourse to individuals in relation to any payments made by them.

While the need to regulate other payment systems in the metaverse (like, blockchain enabled tools other than the digital fiat currency) may be separately assessed, metaverse broadly operates within the scope of existing payment regulations. It must be noted that block chain enabled tools is only one of the many ways in which digital payments or goods can exist in the metaverse.

(iii) ***Users trust on content and services*:** Expansion of metaverse technologies also gives rise to concerns regarding the adequacy of existing legislative frameworks and tools for monitoring the metaverse to identify and filter out illegal and harmful content, given its immersive nature. That said, existing laws governing content moderation will regulate actions on the metaverse as well, when combined default technological measures such as AI-trained detection tools to effectively filter out abuse in the metaverse as well.

Under the IT Act and rules thereunder, intermediaries are required to undertake prescribed due diligence measures; inform users to not display, transmit, publish, or share harmful information or information that is in violation of laws; and disable access to any information that has been flagged in grievances submitted to the intermediary or official communication or order of the government or courts. The proposed Digital India Act also seeks to address content moderation as well in order to address cyber-abuse and protect users and children in digital spaces through regulation of targeted content.

These frameworks, along with provisions under the IPC and POCSO discussed above in addition to other provisions penalising defamation and reputational harm and tort law, will govern a significant portion of content and user actions in the metaverse.

In addition to these legislations, guidelines and protocols/codes for self-regulation will also aid content-moderation efforts in the metaverse – for example, the Guidelines for Prevention of Misleading Advertisements and Endorsements for Misleading Advertisements, 2022 (**Misleading Advertisement Guidelines**) that set out conditions for advertising content, will also apply to advertisements in the metaverse.

Further, various self-regulatory codes and guidelines that serve to regulate content and ensure user safety such as the Code for Self-Regulation (**ASCI Code**) to advertisers that issued by the Advertising Standards Council of India (**ASCI**) also exists.

Independent of such guidelines, metaverse operators are also likely to implement their own measures to regulate content flowing through their platforms, including terms of service informing users of actions that would be violative of laws and the operator's code of conduct, and community guidelines.

(iv) **Data privacy and security:** Please refer above to our response to point (i), (ii) and (iii).

Recommendation 7

- *Based on the feedback received from the industry, we have not found gaps or specific concerns in the existing laws with respect to regulation of the metaverse. There are existing laws, like, information technology, cybersecurity, consumer protection and payment laws along with self-regulatory codes which are applicable to metaverse. Therefore, at this juncture, we cannot recommend that there is a need to develop a regulatory framework for the responsible development and use of metaverse.*

- *Further, the proposed Digital India Act is likely to play a key role in addressing these risks and considerations in regulating the Indian technology landscape. Should there be any gaps between current regulations and challenges emerging in the metaverse, the government can consider addressing them in the proposed law.*

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:

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.

Global practices

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[vi]. 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[vii]. In India, the Government of Telangana has set up a regulatory sandbox for Web 3.0 for innovation in various fields including metaverse[viii].

The introduction of accelerator programs within Centre of Excellences (**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 (**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.

Recommendation 8

- *The ecosystem of regulatory sandboxes (like, experimental campus) should be encouraged, and multiple sandboxes must be set up to assess potential risks and benefits of a new technology, while allowing industry participants the flexibility to reiterate as required.*
- *Accelerator programs should be introduced within the CoEs for industry participants to build partnerships and access resources within the metaverse market.*

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:

India has a strong 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.

Further, the government 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 DoT 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.

This paradigm shift has led countries across the globe to proactively formulate strategic approaches to leverage the metaverse's growth.[ix]:

Recommendation 9

- *Requirements in relation to the Mandatory Testing and Certification of Telecom Equipment by the DoT 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.*

- *The government, industry participants, civil society, technology experts, users, and other relevant stakeholders should collaborate in various ways to determine how the metaverse is governed, for enabling sharing of information and best practices, and developing joint standards or guidelines for effective governance.*

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.

Please see response to Q no 19.

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:

The Electronics and Information Technology Division council (**LITDC**) at the Bureau of Indian Standards, recently established a new panel on metaverse. The scope of the metaverse panel is liaising, investigating the needs for standardisation in the area of metaverse, considering current research, technology and standardisation activities, and trends and recommend an initial roadmap for standardisation activities in the area of metaverse. The endeavour of policy makers should be to support industry-led, consensus-based multi-stakeholder approaches to the development of technology standards.

Moreover, given the critical role that technical standards have in ensuring interoperability and reducing access barriers in the metaverse, it is essential for Indian regulators to introduce policy initiatives promoting active participation from Indian stakeholders in the global standard-setting process. Formulation and implementation of protocols and standards at a global level through cooperation among various stakeholders to govern the metaverse is essential in enabling interoperability.

The ITU, in recognition of the need to have technical standards for the metaverse in place, has constituted the ITU-T Focus Group on metaverse (**FG-MV**). Its eight working groups focus on aspects like applications, interoperability, security, regulatory aspects, sustainability, and accessibility, aiming to lay the groundwork for metaverse services and standards. Other bodies, such as the Metaverse Standards Forum have also commenced multi-stakeholder collaborative processes to work on standards for enabling interoperability in the metaverse at a global level.

Recommendation 10

The government must undertake a more proactive approach through greater participation in these standard-setting processes to ensure that India plays an important role in the formulation of international governance rules and standards.

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?

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 TO Q NO 21 & 22:

Please refer to our response to Q no 17. There are existing laws, self-regulatory codes and guidelines for safety, security, and content moderation in the meta verse. At present, there is need to establish a regulatory framework for content moderation in the metaverse.

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:

Existing laws enable 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, EU and the Indian Trademark Registry (application filed for registration of trademarks in relation to 'downloadable virtual goods' and online virtual services).[x]

For example, EU has clarified that virtual goods in the metaverse can be placed in the existing classification system for trademark registration. Similar guidance was published by the UK IP Office as well. In the US, one judgement applied the existing legal principles of fair use to decide on a copyright infringement claim over a video-game character. Similarly, leading players in the market have made patent filings and secured registrations for metaverse-related technologies such as VR, chips, and operating systems.

As far as enforcement of IPR is concerned, it 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 and dedicated task forces for the metaverse.

For instance, the CP states that there could be jurisdiction complications in the case of metaverse (**Para 4.80**). While this is true but similar jurisdictional concerns have existed in the context of online platforms where IPR infringement issue has arisen beyond the territorial jurisdiction. Likewise, in the case of *Swami Ramdev and Anr. v Facebook Inc and Ors*. the Delhi High Court ordered take down of defamatory videos globally, if uploaded from India. For uploads from outside India, the court ordered platforms to geo-block content to ensure that users from India were unable to access the content.

While this judgment was not related to IP rights, similar principles may be applied in infringement actions in the metaverse. Moreover, from the information provided in the CP, it is not very clear how the jurisdictional issue is unique to the case of metaverse.

Since the meta verse technology is advancing world-wide, efforts are being undertaken in the context of emerging issues in IPR in the metaverse. For instance, early in 2023 the Seventh Session of the WIPO Conversation looked at the wide spectrum of frontier technologies and discussed the challenges the metaverse could pose to the existing IP system. Similarly, 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.

India should lead and participate in global conversations 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.

Recommendation 11

- *We have not received feedback from stakeholders highlighting any specific concern or challenge in terms of registration of IPR in metaverse or enforcement/protection of IPR in the metaverse, interoperability and compatibility of IPRs across different virtual environments which may require modification to the existing IPR framework. Hence, we cannot recommend any modification to the existing IPR framework.*

- *When any such specific IPR challenge or risk arises and brought to our notice, questions like, whether the concerned issue is related to the Trademarks Act, Copyright Act or Patents Act; what exactly the nature of concern is, which provision of the given law needs to be analysed, whether it can be addressed through issuance of guidance/FAQs or through parliamentary intervention, could be examined on a case-to-case basis.*

- *We recommend that India should participate in global conversations and multi-stakeholder's approach in various IPR issues around metaverse including interoperability and compatibility of IPRs across different virtual environments.*

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:

As highlighted in the TRAI White Paper, the 6 GHz band is much wider than the 2.4 GHz and 5 GHz bands and supports low latency, high throughput, security services and better speeds. These features are critical for the metaverse which involve multiple users and congested networks. Wider channels also enable a better user experience and longer battery life for AR/VR head mounted displays.

However, use of the 6 GHz band is currently limited, as it is a licensed band in India. Internationally, almost 35 countries have chosen to delicense the 6 GHz. The rationale for delicensing has been to enhance benefits to citizens while reaping the benefits of economic growth in their economies. In this context, we can refer to the recent estimation done by Prof. Rekha Jain from the IIM-A that the economic value of unlicensed spectrum bands in India is significant for 2025: INR 12,69,998 crores (for GDP at current prices). This is nearly 6% of the projected GDP in 2025. The contribution of the 6 GHz band is expected to be 9.5% to the total economic value in 2025 (The Economic Value of wi-fi spectrum for India). Another study conducted by the NIPFP in 2018, although in the context of E-band & V-band, illustrates the economic benefits generated by certain unlicensed spectrum.

Consumer Unity & Trust Society (**CUTS**) in its study of global experience of regulatory approach towards 6Ghz (*See, Annexure 1, page 11-14*), shows economies from the **global south** where nations like **Brazil, Colombia and Peru** have fully opened the 6 GHz band for Wi-Fi use. Broadly, the rationale of these nations to open up 6 GHz includes boost to local economy by unlocking full potential of Wi-Fi 6E to give consumers the best connectivity experience, develop an entire ecosystem around 6 GHz, provide higher transmission rates, decongest mobile connectivity, better multiple access experience, alignment with international practices.

For instance, this recent 2020 study assesses the **GDP contribution of allocating 1200 MHz in 6 GHz band** for the **Brazilian economy**. The study projects that deployment of **IoT and AR/VR solutions** can together generate approximately 54 USD billion between 2020-30. Total GDP projection between 2020-2030 is approximately 112 USD billion which is broadly attributable to increased speed, enhanced capability for cellular off-loading, enhanced capability for cellular off-loading/decongestion, wide deployment of IoT, AR/VR, etc.

Recommendation 12

Based on the feedback received from industry, we recommend that the government may consider delicensing 6Ghz for wider economic benefits, including to spur the growth of metaverse ecosystem. This recommendation aligns with scenario 2 – unlicensed, as one of the regulatory options suggested by the TRAI in its white paper on 6 GHz band. In case there are specific concerns with delicensing these should be separately discussed, and a decision taken in the overall economic interest.

For any queries related to this submission, please contact:

Ashish Aggarwal (asaggarwal@nasscom.in) or Sudipto Banerjee (sudipto@nasscom.in) with a copy to policy@nasscom.in.

About nasscom

Nasscom is the premier trade body and chamber of commerce of the Tech industry in India and comprises over 3000 member companies including both Indian and multinational organisations that have a presence in India. Established in 1988, nasscom helps the technology products and services industry in India to be trustworthy and innovative across the globe. Our membership spans across the entire spectrum of the industry from start-ups to multinationals and from products to services, Global Service Centres to Engineering firms. Guided by India's vision to become a leading digital economy globally, nasscom focuses on accelerating the pace of transformation of the industry to emerge as the preferred enablers for global digital transformation. For more details, kindly visit www.nasscom.in

[i] See here: https://www.trai.gov.in/sites/default/files/CP_29092023.pdf

[ii] 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. For example, courts in the U.S. and EU respectively, have treated non-fungible tokens (**NFTs**) and creations in the metaverse as artistic works and protectable by copyright. The latest Nice Classification[ii] now includes "downloadable digital files verified by NFTs" under class 9.

- For the U.S. - Hermes International et al v. Rothschild, United States District Court, S.D. New York, 18 May 2022.
- See here for EU. In a judgment from the ECJ, the court stated that although these creations cannot be considered as computer programs they can be considered as artistic works, thus be protectable by copyright, as long as such interface is the author's own intellectual creation.
- International Classification of Goods and Services for the Purposes of the Registration of Marks under the Nice Agreement.

[iii] https://www.tec.gov.in/pdf/M2M/Securing%20Consumer%20IoT%20_Code%20of%20pratice.pdf

[iv] https://dot.gov.in/sites/default/files/Advisory%20Guidelines%20to%20M2M_IoT%20stakeholders%20for%20secring%20Consumer%20IoT_1.pdf

[v] Sections 354A, 354D, Indian Penal Code; Sections 67, 67A, IT Act.

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

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

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

[ix]
- China recently announced a three-year action plan for development of the metaverse industry,
- 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'.
- South Korean government has announced a $186.7 million package (as part of the Digital New Deal program) to simulate a government led metaverse ecosystem.

[x] 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. For example, courts in the U.S. and EU respectively, have treated non-fungible tokens (**NFTs**) and creations in the metaverse as artistic works and protectable by copyright. The latest Nice Classification[x] now includes "downloadable digital files verified by NFTs" under class 9.

- For the U.S. - Hermes International et al v. Rothschild, United States District Court, S.D. New York, 18 May 2022.
- See here for EU. In a judgment from the ECJ, the court stated that although these creations cannot be considered as computer programs they can be considered as artistic works, thus be protectable by copyright, as long as such interface is the author's own intellectual creation.
- International Classification of Goods and Services for the Purposes of the Registration of Marks under the Nice Agreement.