Response to India’s Strategy for National Open Digital Ecosystems (NODE) Whitepaper

Submission by The Dialogue

Authors: Ayush Tripathi, Karthik V Venkatesh, Kazim Rizvi, Shefali Mehta, Trisha Pande

Research Assistance: Eshani Vaidya

1. Introduction

The Open Data Movement across the world aims to harness the power of big data, which has traditionally been used by the private sector, and leverage it into systems which help citizens adopt easier ways of performing everyday tasks such as making payments, accessing public delivery services and allow public policy to be more informed. With this context in mind, we are grateful to the Ministry of Electronics and Information Technology (MeitY) for allowing civil society to respond to their whitepaper on 'National Open Digital Ecosystems' (NODE).

At the Dialogue, we believe in the transformative power of technology to ensure that society can be changed for better. We try to engage with citizens and stakeholders on matters that affect them in a rapidly advancing technological world, with the long term objective of driving sustainable reforms through informed public opinion and citizenry participation. Data as a resource has the potential to define new futures, improve our standards of living, foster innovation and accelerate inclusion. Technology and societal change needs to include every stakeholder and beneficiary, and must be set on a strong framework of rights.

We believe that the current framework for NODE ties squarely with our mission statement. NODEs are defined as open and secure digital delivery platforms, anchored by transparent governance mechanisms that enable community of partners to unlock innovative solutions, to transform societal outcomes[1]. As the government is preparing to make a paradigm shift to Govtech 3.0, and come up with a national strategy in this regard, we find that there are a few crucial points that need further deliberation and consultation.

[1] Ministry of Electronics and Information Technology. (2020). *Strategy for National Open Digital Ecosystem (NODE): Consultation White Paper*. Retrieved from https://static.mygov.in/rest/s3fs-public/mygov_158219311451553221.pdf

We have identified the following as the main issues that need further scrutiny:

1. Clearly define the standards of openness that will be adopted by the NODES
2. Making datasets available and accessible to all
3. Creating an interactive and evolving digital platform for feedback of NODE ecosystems
4. Localizing monitoring the regulation of NODE ecosystems
5. A strong data protection law, and a regulation regarding Non personal data must be put in place before the national strategy is finalised to harmonise the laws, and ensure rights of stakeholders are secure.

At The Dialogue we are committed to supporting the government towards this initiative and look forward to working closely with the Ministry of IT and other relevant stakeholders towards the same.

2. Principles of the NODE

[A] **Principle -1:** Be open and interoperable

The white paper has provided the definition for the term “open” as an inclusive list involving accessibility, transparency, open API standards and open source code. However, the paper also iterates that the degree of openness will vary with each node. In order to have maximum transparency, ***firstly***, *it is important to set minimum standards for openness*. Krechmer has suggested 10 criteria for assessing the openness of standards which could be used as a best practice for the government.[2] The degree of such standards should be made only after setting a bare minimum standards for openness that all NODE should comply with.

The openness of each NODE must comply with the directives and policy of the government including the **policy on adoption of open source software.**[3] This policy was framed to shift the focus from closed door software to an open source which will help in achieving the objective of enabling transparency. Therefore, clear standards[4] openness must be defined as a common practice, with increased reliance on open movements across the globe and many governments are tapping benefits from this.

Secondly, in order to ensure accountability, **there needs to be a clear public explanation if certain NODES decide to not opt for the same degree of openness prescribed.** Any exception in this regard will dilute the principles of openness and transparency.

[2] Krechmer, K. (2009). Open standards: A call for change. *IEEE Communications Magazine*, *47*(5), 88-94. doi: 10.1109/mcom.2009.4939282

[3] Ministry of Communication & Information Technology. (2014). *Policy on Adoption of Open Source Software for Government of India*. Retrieved from https://meity.gov.in/writereaddata/files/policy_on_adoption_of_oss.pdf

[4] Ministry of Communications & Information Technology. Policy on Open Standards for e-Governance (2010).

Thirdly, interoperability has been one of the long standing issues in the e-governance architecture. The white paper does not provide the means through which such interoperability will be achieved. However, the government has an interoperability framework on e-governance[5], it's use in the NODE is still doubtful. Technology will not be much of a problem in interoperability in comparison to the organisation challenges. To ensure smooth interoperability, state and central cooperation will be needed. Further, the government will face challenges such **as redefining rules and procedures, information transparency, legal issues, infrastructure, skill and awareness, access to right information, interdepartmental collaboration and the tendency to resist the change in work culture.**[6] It is important that these issues are addressed to prevent implementational haphazard.

[B] Principle - 2: Make Reusable And Shareable

This is an important part of a digital ecosystem however, the **reusability must be tested on the basis of purpose limitation and data must be shared only after obtaining the consent of the data principals**. Inclusion of public participation and knowledge is crucial to the success of NODE. An online consent mechanism must be developed prior to the implementation of NODE which should be a public authority in order to make them accountable for any breach.

[C] Principle - 4: Privacy And Security

In the absence of a data protection law in the country to ensure accountability, it is very important to ensure privacy and security of the NODE and the stakeholders there. While it is highly recommended that the data protection laws and regulations are to be put in place before the implementation of the NODE, we strongly believe that every move to operationalise the

[5] Ministry of Communications and Information Technology. Interoperability Framework for e-Governance (2015).

[6] Shrivastava, S., Pandey, A., & Kumar, P. (2010). Interoperability issues for E-Governance Framework. *International Journal Of Information Technology & Knowledge Management*. doi: http://csjournals.com/IJITKM/Special1/10.%20Interoperability%20issues%20for%20E-Governance.pdf

NODE must be rooted in principles of data protection. To that end, we analyse privacy and security standards.

[C.1.] Privacy Standards

The white paper does not provide the exhaustive list for standards that will be incorporated in the system however, it is important that NODE comes with **principles of privacy with design being observed to its core**. General Data Protection Regulation identifies six privacy principles i.e. lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy of data; data storage and identity and confidentiality of the data. These six principles should be at the core of NODE. Further, the whole **NODE should be governed by the principles of necessity, proportionality and legality.**

Further, the data obtained by the system should be **owned by the data principal.** It is important that any objective for commercialisation of this data should not be done without the consent of data principal. As mentioned above, a consent mechanism must be implemented before the government seeks to operate NODE.

The purpose for which data is obtained must be clearly defined. It is important that it does not become a tool of surveillance. To ensure transparency standards, citizens must be given access to their data sets including information with regard to where his/her data is being used and for what purpose. Additionally, the storage of data needs to be impenetrable. Regular monitoring of data and ensuring its legitimate use must also be completed.

We also recommend enabling **regular independent data auditing** of the NODE in order to ensure its compliance with the directives and policies of the government.

[C.2] Security Standards

In the past, government systems have been prone to cyber attacks, therefore maximum security standards have to be observed. For this, the government must look at **cryptography techniques** as one of the options. Further, it is also necessary that centre and state follow the same security standards in order to have better coherence and system maintainability. The impact of a breach in the security of NODE could impact the whole ecosystem because of its interoperable and shareable nature. India has to keep in mind the attack on Estonia's digital ecosystem in 2007 which affected various sectors and crippled the country.[7] There is a need for comprehensive cybersecurity policy measures as a base for any national digital ecosystem to work on.

In order to ensure an effective cybersecurity protocol, there is a need to deploy systems where securities issues are found and fixed proactively.[8] For this, India could also develop a system similar to the National Infrastructure Protection Plan (NIPP) which will help in mitigating the risks. NIPP identifies areas of concern such as interdependencies, cybersecurity and the international nature of threats. It helps in mitigating physical, cyber and human threats. Similarly, keeping in mind large scale deployment of NODE, a committee could be constituted to come up with regular security updates and the possible vulnerabilities and threats that can be used and deployed by the concerned department handling the NODE.

[D] Principle - 6: Accountability

An independent regulatory authority is essential to maintain accountability within the platform created. Such an authority must be autonomous, transparent, consistent with the established goals and practices.[9] Further, it is important to have **decentralised regulatory accountability**. Apart

[7] Priisalu, J., & Ottis, R. (2017). Personal control of privacy and data: Estonian experience. *Health And Technology*, *7*(4), 441-451. doi: 10.1007/s12553-017-0195-1.
[8] IGF 2017 - Best Practice Forum on Cybersecurity. (2020). Retrieved 31 May 2020, from https://www.intgovforum.org/multilingual/content/igf-2017-best-practice-forum-on-cybersecurity.
[9] Bugli Innocenti, E. (2015). *Public Private Partnerships in e-Government Guide*. Kyiv, Ukraine: USAID. Retrieved from http://ppp-ukraine.org/wp-content/uploads/2015/03/PPPs-in-e-Gov-Guide-ENG.pdf.

from a national regulatory body, there is a need for either a state wise or zone wise regulatory bodies to ensure accountability at the last mile delivery of services.

Further, there must be clarity on the guidelines as well as the rules and regulations to be followed to be followed by the regulatory authorities. This would also include highlighting the rights and duties of the stakeholders and the citizens. This can be furthered by drafting formal procedures to be followed by all parties involved.[10] It's important to establish frameworks to appropriately evaluate the performance of the project at all levels of the government, and to uniformly apply standards, guidelines and compliance with interoperability frameworks.[11] These frameworks must also review novel digital opportunities as well as further developments in the laws regulating the same.[12]

[E] Principle 7: Establish Rules of Engagement

Division of the roles and responsibilities by non-government stakeholders require the consideration of different motivations and goals. This exercise helps to identify which actors might be more driven than others adopt a digital ecosystem. For instance, public sector organisations are likely to adopt and maintain the rules of engagement for GovTech 3.0 NODE technology because of their close relationship with the government.[13] Since the private sector must assume the responsibility of certain areas when building an effective system of e-governance such as the NODE by putting in its time and resources, the success of the ecosystem is central to dividing responsibility.

[10] Public Governance Committee. (2014). *Recommendation of the Council on Digital Government Strategies*. OECD. Retrieved from https://www.oecd.org/gov/digital-government/Recommendation-digital-government-strategies.pdf.

[11] *Id.*

[12] *Id.*

[13] Ashaye, O., & Irani, Z. (2019). The role of stakeholders in the effective use of e-government resources in public services. *International Journal Of Information Management*, *49*, 253-270. doi: 10.1016/j.ijinfomgt.2019.05.016

Different levels of risk are associated with the roles and responsibilities assumed by stakeholders in the ecosystem. In order to ensure that conflict is minimized and responsibilities are performed smoothly, the following approaches may be undertaken

[E.1] Regulatory Commission by Local Administration

Establishing local bodies at a district level which oversee how stakeholders are committing to their responsibilities can be an effective method of monitoring the impact on public services. The body could have local government officials across departments as board members.[14] The purpose of setting up such a regulatory commission is to establish a strong and independent regulator at the **local** level to measure and assess the impact of a Public-Private Partnership (PPP) on the lives of citizens. Mismanagement due to political influence[15] will be reduced and helps to establish local capacity - which is a key factor in making a system under NODE widely adopted.

[E.2] Contract Structuring

As the study of Ukraine on PPP in e-governance reveals, the manner in which the contract is framed for the stakeholders in the ecosystem determines the outcomes and success of the project. Therefore, there is a need to focus on parameters such as **outlining monitoring clauses -** who is responsible for evaluating the technical performance of partners, areas where tariffs are applicable, reporting of data usage under the open ecosystem etc and including **dispute resolution measures** in the contract - under what circumstances the contract can be renegotiated, which third party is assigned to arbitrate, and under what circumstances the government or private entity is allowed to default on the contract.[16]

[14] infoDev Communications & Publications. (2009). *Public-Private Partnerships in E-Government: Handbook.*

[15] Water Regulation: Separate Regulatory Body with Licensing Regime | Public private partnership. (2019). Retrieved 31 May 2020, from https://ppp.worldbank.org/public-private-partnership/water-regulation-separate-regulatory-body-licensing-regime

[16] *Supra* note 7.

[E.3] Capacity Building and Resource Allocation for Contracting Authority

One of the pitfalls of an ecosystem with private and public stakeholders is that the contractual obligations are dependent on the oversight of the contracting authority. Since some private players might have more of an advantage by way of using their legal resources, it is important to equip and build capacity for negotiation. These negotiations and dialogues are important for the public and private sector in order to reduce monopolization of responsibility by any one stakeholder. Since PPP contracts in a sector as evolving as e-governance change with emerging technology, consultant assistance can be used in order to have discussions which contribute to a common vision for the ecosystem under consideration.[17]

[F] **Principle 8:** Create Transparent Data Governance

Ensuring transparency and accountability in data governance is largely dependable on emphasizing easy availability and making it free of cost to avail. There are examples from countries such as Kenya, where the national Open Governance Data Initiative did not work as expected. The number of users of the platform remained static, and actually decreased.[18] There is a need to delve into contextual examples from other developing and developed countries to better understand the principles to making data open and accessible for end users, and the pitfalls India must avoid.

[F.1] Availability and Accessibility of Datasets

It is necessary that the data are available to users in a disaggregated format, and in an electronic format that is usable. In data collected from different districts, subdistricts, villages, blocks etc. there needs to be uniformity. It is important for the data to be in the **correct electronic format -**

[17] *Id.*

[18] Lwanga-Ntale, C., Mugambe, B., Sabiti, B., & Nganwa, P. (2014). *Understanding How Open Data Could Impact Resource Allocation for Poverty Eradication in Kenya and Uganda*. Retrieved from http://www.opendataresearch.org/sites/default/files/publications/Open%20Data%20for%20Poverty%20Eradication%20-%20DRAFT.pdf.

often, the data is found in PDFs and although it is electronic and can be read by a human. However, on a computer it is not possible to analyse it using computer software. Therefore, care must be taken to ensure that the data is in a **convenient** and **modifiable** form. Government departments should be encouraged to adopt certain software such as MS Excel and Google Sheets and record their data on it, as well as encourage them to understand different kinds of formats and standardise their data collection.

The following parameters[19] must be embedded to ensure availability and accessibility -

1. Be in **machine readable** formats,
2. Must not require specific softwares to use it, must be in an open format,
3. Identify the most important datasets integral for public use, and release more than a few subsets of that data for **bulk downloads,**
4. Released in a **timely fashion,**
5. Establish structured relationships between different datasets.

[F.2] Devise an App which Allows Civil Society and Government to Collaborate

European public administration is ensuring that there are efficient and quick communication channels between the government and civil society by way of 'apps for democracy'. These apps allow voters to engage meaningfully with their government on the count of data ecosystems and they can flag concerns or suggest improvements. Clearly marked information about the ecosystem can also help increase trust and foster a clearer understanding of political systems.[20] Applications which provide citizens with real-time information, using online platforms to crowdsource ideas, and testing algorithms to engage communities in day-today administration

[19] OECD. (2013). *Open Government Data: Towards Empirical Analysis of Open Government Data Initiatives*. Retrieved from https://www.oecd-ilibrary.org/docserver/5k46bj4f03s7-en.pdf?expires=1590936517&id=id&accname=guest&checksum=B2A36E885A17527727D4F6D6C97CEB8C

[20] Ross, E. (2020). Apps for democracy – open data and the future of politics. Retrieved 31 May 2020, from https://www.theguardian.com/media-network/2016/aug/19/apps-for-democracy-open-data-and-the-future-of-politics

have been experimented with in Europe under the category of '**digital democracy**' and could be beneficial for India too, under the umbrella of NODE.[21]

An example of such participation is France's Le Grand Debat National which is a platform where users can log on and debate questions essential for the country. Themes are divided which ask citizens to submit their responses - themes include ecology, taxation, democracy and the organization of state and public services. For greater visibility of the tools and to make them accessible universally a digital platform is established. A toll-free number accompanies the platform and allows those who wish to have information or clarification on all the questions concerning the great debate.[22] India can replicate this system to discuss themes within the NODE at a later stage.

[G] **Principle 10:** Adapt a Suitable Financing Model

The principle in its current form is very vague. However, in the past the government has shown the intent to monetise the data through its sale to private entities.[23] Monetisation of data should be done in accordance with a framework which will specifically mention the categories of data that could be monetised across departments. However, it must be ensured that personal data is not used for the purpose of monetisation. There is a need to come up with a financing model which has a joint effort of public and private partnerships which could be ideally suited for this scenario. However, to ensure accountability and transparency, relevant authority **should disclose sources and amounts of funding, and budget execution for each NODE.**

[21] European Parliament. (2020). *Digital democracy: Is the Future of Civic Engagement Online?*. European Parliament Think Tank. Retrieved from https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/646161/EPRS_BRI(2020)646161_EN.pdf

[22] Le Grand Débat National. (2020). Retrieved 31 May 2020, from https://granddebat.fr/

[23] Nath, D. (2019). Ministry plans to go from open platform to eventual monetisation of cities' data. Retrieved 31 May 2020, from https://www.thehindu.com/news/national/ministry-plans-to-go-from-open-platform-to-eventual-monetisation-of-cities-data/article29385873.ece

[H] **Principle 15:** Grievance Redressal Mechanism

Grievance redressal mechanism should be a multi staged process that must be resolved within a **specific timeline**. Small technical grievances could be raised on a mobile application software which should be resolved within 24 hrs. It is important to ensure that the constitutional and legal rights guaranteeing access to critical government services are not replaced with internal mechanisms governed merely by standard operating procedures. Therefore, Grievance related to data protection and breach of trust should be linked to the independent Data Protection Authority under Personal Data Protection Bill, 2019 and appellable procedure should be opted for. On a non judicial front, the government could look at the exploratory analysis prepared by University of Manchester on non-state based non judicial grievance mechanisms.[24]

[24] Dr. Zagelmeyer S., et.al., "Non-state based non-judicial grievance mechanisms (NSBGM): An exploratory analysis", University of Manchester. https://www.ohchr.org/Documents/Issues/Business/ARP/ManchesterStudy.pdf.

3. Delivery Platforms

In understanding the design behind the delivery platform that would be appropriate for NODE, we believe that it is crucial to move towards an open governance model and unlocking potential solutions and economic benefits. The whitepaper has set four technological structures the NODES could take[25], and the four types have varying degrees of benefits in enabling an ecosystem. As per the government policy on open source governance[26], the move to tap the benefit with community involvement is welcome.

An important feature of enabling an effective digital ecosystem, is the *seamless flow of data, and interoperability*. Towards this, there needs to be a clear mapping of the various departments involved, and interactions. Integration is defined as a multidimensional process comprising two distinct processes of interactions and collaboration.[27] Interaction represents the structural nature of cross departmental activities. These are systemic processes that exist to ensure that there is synergy within the functioning of various government departments. Collaboration involves the unrepresented, affective nature of interdepartmental relationships. This would require the departments to work towards a common goal, with a shared vision. There needs to be integration of the various information systems currently in place. Mapping out the inadequacies based on an agreed upon standard can be beneficial in this regard. An audit of each department, and the systems will allow us to formulate the plans better for addressing the inadequacies/barriers in building a digital ecosystem.

[25] *Supra* note 1.
[26] Ministry of Science and Technology. National Data Sharing and Accessibility Policy (2012).
[27] Kahn, K. (1996). Interdepartmental Integration: A Definition with Implications for Product Development Performance. *Journal Of Product Innovation Management*, *13*(2), 137-151. doi: 10.1111/1540-5885.1320137.

The white paper mentions that there will be sector specific NODEs that will be defined later. Towards this, the data that are currently operating in silos need to be streamlined in a standardised format that can be transferred. The Ministry/Department that is building the NODE will be looking over the development. It is crucial to flag areas of intersection, and liaison closely with the other areas the NODE might steer into. For example, in a Health Node, which will come under the ambit of the Ministry of Health and Family welfare, the ecosystem might include insurance companies, that fall typically under the ministry of finance. To that extent, proactive identification of intersections, and cross departmental integration is crucial.

To maximize the benefits we rely on sharing and reusing definitions and terms. As part of the principles enumerated in the Whitepaper, Govtech 3.0 will rely on reusable and interoperable data. Data quality and data governance issues need to be addressed to ensure a coherent operation on data of known and monitored quality.[28] This becomes crucial to scaling and finding effective solutions. A quality framework specifying the particulars for every NODE should be followed by a data audit. The Data audit will look into the availability of the data, and matches it with the particulars of the quality framework.. For future purposes, strict norms on collection and storage of data can bring about standardisation and cohesion. Initial investment in these processes can result in cost savings subsequently.

Finally, in view of securing the rights of the platform- the data privacy and security must be ensured. The whitepaper is unclear on the specifics of what data would be collected, shared and stored. Depending on the nature of data, the harm to the citizen/business/community might be drastically different. In the conceptualisation of platforms, due importance must be given to considerations of privacy, and technical safeguards against data breaches. Strong encryption standards, and anonymisation protocols for personal data must be followed in synergy with the Personal Data Protection Bill. The Committee that is currently looking into the regulation of Non

[28] Myrseth, P., Stang, J., & Dalberg, V. (2011). A data quality framework applied to e-government metadata: A prerequisite to establish governance of interoperable e-services.

Personal Data must also define standards to be followed while using it for public good. More on this is elaborated in [C.1] and [C.2]

Recommendations:

- Develop a quality framework to assess data usability and quality prior to the deployment of NODE
- Increase interdepartmental cooperation for effective functioning of NODE. Prior to the launch of a platform for the NODE, clear mapping of the deficiencies in the information systems must be undertaken.
- Engage with the community to make the data accessible

[A] <u>Question 3</u>

What are the biggest challenges that may be faced in migrating from a 'GovTech' 1.0 or 2.0 approach to a NODE approach (e.g. interdepartmental systems integration, legacy systems modernization, poor usability, and poor data quality)? How might these be overcome?

In addition to the problems enumerated above, sustained effort must be given in bridging the digital divide. To maximise service delivery, and foster innovation pan India, more individuals need to be onboarded and provided digital literacy to use these digital public infrastructure. Additionally more clarity on what data each NODE will associate with must be clearly defined earlier, with clearly laid out access protocols, and terms and conditions for data sharing. This will allow for oversight of the activities that are carried out with data, transparency and accountability. Caution must also be taken in cybersecurity risks that will be associated with the integration of departmental databases and modernisation of legacy systems.

4. Governance

[A] <u>Question 5:</u>

Do NODEs across sectors require common governance frameworks and regulatory/ advisory institutions to uphold these? Or is it sufficient for each node to have an individual governance construct? If a common framework is required, please elaborate the relevant themes/ topics e.g. financing, procurement, data sharing.

Chapter IX of the Personal Data Protection Bill 2019 establishes the presence of a Data Protection Authority. Clause 41 (4) details that *the Authority may, with the prior approval of the Central Government, establish its offices at other places in India*[29]*.* In this regard, the envisaged Data Protection Authority can act as a regulatory institution for NODE frameworks. Offices that are set up in states can establish their presence in districts and coordinate with them - synthesizing efforts of the Centre and states.

The concerns to be addressed are as follows -

1. **Preparedness** - The first exercise to be undertaken for an ecosystem under NODE should be to map out areas and assess them on their preparedness levels for Open Data. This can be in the form of an interactive data visualization on the proposed interactive website (detailed under Principle 8 in this response paper) and can allow inputs from local citizens along certain metrics - such as **People** (e.g. skills, capabilities, etc.), **Processes** (workflows, data normalization, data sanitization, etc.) and **Technology** (e.g. tools, platforms, portals, etc.)[30]

2. **A common programme for procurement** - India can consider a common procurement

[29] The Personal Data Protection Bill (2019).

[30] Tata Trusts. (2019). *Open Data Urban India Frame Implementation Guidelines*. Retrieved from https://www.tatatrusts.org/upload/pdf/open-data-urban-india-frame-implementation-guidelines.pdf.

program and devise it with the help of civil society and cybersecurity government experts, which allows for standardization of security assessment, authorization, and continuous monitoring for cloud products and services. The United States of America uses the **Federal Risk and Authorization Management Program (FedRAMP)** for this purpose, which saves an estimated 30-40% of government costs, as well as both time and staff required to conduct redundant agency security assessments. FedRAMP is the result of close collaboration with cybersecurity and cloud experts from the General Services Administration (GSA), National Institute of Standards and Technology (NIST), Department of Homeland Security (DHS), Department of Defense (DOD), National Security Agency (NSA), Office of Management and Budget (OMB), the Federal Chief Information Officer (CIO) Council and its working groups, as well as private industry.[31]

3. Encouraging Open Data Use Agreements - India should consider partnerships such as the **Open Data Policy Lab** and **GovLab** which creates an ecology in which governments can engage with industry to identify data that may be useful in addressing important public policy issues.[32] This partnership between Microsoft and New York University[33] encourages the inclusion of toolkits, frameworks and best practices to support data sharing and data-driven decision-making and builds a community of data stewards and other data stakeholders within the public and private sectors.

[B] Question 6:

Are you aware of any innovative financing models that could be deployed to build NODEs? If yes, please describe along with examples e.g. PPP models or community crowdfunding models

[31] FEDRAMP | OLAO. (2020). Retrieved 31 May 2020, from https://olao.od.nih.gov/content/fedramp.
[32] Open Data Policy Lab. (2020). Retrieved 31 May 2020, from https://opendatapolicylab.org/.
[33] Yokoyama, J. (2020). Closing the data divide: the need for open data - Microsoft on the Issues. Retrieved 31 May 2020, from https://blogs.microsoft.com/on-the-issues/2020/04/21/open-data-campaign-divide/.

Crowdfunding initiatives, while attractive, do not have the capacity to fund projects under NODEs because they aren't viable in the long term. NODEs require significant financial support, not only for maintenance, but also to foster Research and Development. Public-Private Partnership (PPP) models are the ideal choice with regards to NODE's for several reasons: the risk is borne by the party that is best suited to manage the same; allows for innovation and growth; for development of independent revenue streams and engagement of technology experts and professionals.

For example, the Common Service Centres (CSC) project aimed at establishing service centres that would allow people in rural and remote areas to access government services.[34] This project had a variety of revenue streams, such as subscription services, government services for citizens, business to business services among several others. However, the project couldn't incentivise development because the minimum support provided by the government was not based on the services rendered or output delivered. Instead, the government guaranteed minimum support per month for the first three years.[35] Therefore, it's important to modify each financial model based on the unique needs of every platform or service provided.

In order to have an effective PPP, the principles of transparency and accountability must be expressly outlined. It is also important to maintain a list of all the on-going digital initiatives to avoid duplication of data sets and systems.[36] The allocation of funds, budget, over or under-utilisation of funds etc. must be information that is easily accessible to maintain the democracy of the proceedings. Allowing people to be familiar with the financial plans allows the building of public trust and leads to more informed decision making by the stakeholders. For example, every time the overall cost of a project exceeds the established budget *x*, the expected

[34] Ojha, S., & Pandey, I. (2017). Management and financing of e-Government projects in India: Does financing strategy add value?. *IIMB Management Review*, *29*(2), 90-108. doi: 10.1016/j.iimb.2017.04.002.
[35] *Id.*
[36] Public Governance Committee. (2014). *Recommendation of the Council on Digital Government Strategies*. OECD. Retrieved from https://www.oecd.org/gov/digital-government/Recommendation-digital-government-strategies.pdf

socio-economic benefits should be highlighted to justify public spending.[37] It's important that the financial strategy is open and accessible because it has a direct effect on strategic management and the eventual success of the project.[38]

For example, Singapore deployed an e-Procurement Project to provide a one-stop solution for all government procurements. This model has been widely acknowledged as a model "PPP in Government" project globally. The procurement cell evaluates bids from suppliers and then makes a selection on the basis of specific requirements that are communicated to them via a government agency. This procurement cell helps eliminate the scope for corrupt practices because it doesn't allow any government agencies seeking the procurement to be involved in the analysis part of the process. The project clearly defines the roles of each stakeholder, and outsourced all the technical services. The government, however, has sole control over ensuring that the project is in compliance with the laws and regulations.[39] Ukraine has attempted to develop a 'Public-Private Partnership Development Program' in order to create a regulatory and legal framework around PPP's.[40] Similarly, the U.K. government's policy requires that a PPP must generate allocative and productive efficiency that is superior to a traditional financial model.

Every single financial model, PPP or otherwise, must finance a data protection team that would consist of a Chief Privacy Officer, an Open Data Team and Department Data or Privacy Officer. Their duties should include, but not be limited to, engaging the public about data and privacy, determining how data should be released, evaluating the ecosystem of data available on portals, ensuring that the datasets being released have thorough metadata that describe any protections

[37] *Id.*
[38] *Id.*
[39] Sharma, S. (2007). Exploring best practices in public–private partnership (PPP) in e-Government through select Asian case studies. The International Information & Library Review, 39, 203-210.
[40] *Supra* note 7.

taken to protect privacy in the data.[41] An independent regulator must also be constituted to ensure accountability, transparency, autonomy and consistency.[42]

[C] <u>Question 7:</u>

What are some potential risks that open digital ecosystems can leave citizens vulnerable to, for example, risks related to data privacy, exclusion, having agency over the use of their data etc.? What types of overarching guidelines and/or regulatory frameworks are required to help mitigate them?

Open digital ecosystems increase citizen vulnerability because they involve all things data. Data is collected at various stages of the development, maintenance and operation of the various platforms that would constitute the digital ecosystems. The increased exposure brings up several concerns relating to privacy, competition law, intellectual property rights and overall data protection.

[C.1] Data Protection

Data protection not only concerns itself with mitigating risks of attacks or leakages. It extends to public expectations with regards to state management of data, collection, storage and/or publication of data not only increasing vulnerabilities among citizens, but also leading to an increase in criminal activity or poor policy making. Data, therefore, must be protected at every single stage--collection, transfer, publication as well as storage.

[C.1.1] Data Collection

Among the several factors to consider while collecting public data, the most prominent include---purpose of data collection i.e. why the data is crucial; would the data pose the risk of

[41] Green, B., Cunningham, G., Ekblaw, A., Kominers, P., Linzer, A., & Crawford, S. (2017). *Open Data Privacy*. Berkman Klein Center for Internet & Society Research Publication. Retrieved from https://dash.harvard.edu/bitstream/handle/1/30340010/OpenDataPrivacy.pdf.

[42] *Supra* note 27.

re-identification; public expectations about acceptable government data collection; and whether or not the data would be made a part of public record. For example, addresses of pedestrians pose a high risk of re-identification and violation of public trust, and should not be published on open source platforms. For example, the names and addresses of several people having testing positive for COVID-19 were released in Delhi, Chandigarh, Ajmer and other areas. This was a serious violation of the individual's right to privacy, as well as a violation of public trust.[43]

The manner of data collection within India also needs drastic improvements. Census data, for example, is collected every 10 years, which leads to several policies being drafted on the basis of a Census that would be outdated. With the establishment of NODEs, the collection of data would take place from a variety of sources. It’s important that the data is understandable, easily available, and is consistent in its format so as to be reliable indicators of change. In order to ensure that the data collected by the government through questionnaires is accurate, the data collection should take place in a more routine manner at the ward level. This would not only provide researchers with updated and relevant information, but would also allow them to come up with concrete analyses based on this data.

Most importantly, the reasons for collection of data must be specified along with very clear information regarding how the data is not going to be used. This will allow for a greater degree of transparency, openness and public trust building.[44]

[C.1.2] Classification and Publication of Data

Classification of data acts as a determinant of collection, storage, maintenance, publication and deletion of data. For example, management of open data, such as a public transport schedule will

[43] Jaiswal, P. (2020). Privacy of COVID-19 suspects violated; names, addresses made public. Retrieved 31 May 2020, from https://www.theweek.in/news/india/2020/03/22/privacy-of-covid-19-suspects-violated-names-addresses-made-public.html.

[44] *Supra* note 41.

vastly differ from the management of closed data, such as employment contracts. It therefore plays a pivotal role in securing one's privacy. Another risk posed to individual privacy is that developments in data analytics are growing at such a rapid pace, that while the data may remain the same, the risks are ever changing.[45]

For example, photographs can be used in unpredictable ways.[46] Unlike structured data fields, where each entry takes on a specific predetermined value, unstructured fields are those that include data that do not have accounted for data. Examples include photographs, certain comments, descriptions etc. In 2012, Philadelphia, U.S.A. published gun permit applications online as a part of their open data initiative. Each applicant was required to provide their reason for application.[47] Several applicants entered "carrying large sums of cash at night" in that field, which created a "roadmap for criminals" according to a lawyer that fought the class action lawsuit against the City.[48] Therefore, before publication of such data, it would be beneficial to remove the unstructured fields entirely.

A tiered approach must be employed while publishing data. Classification of data, i.e. the kind of data set one seeks to publish, will determine the decision to publish, as well as the manner of publishing. The Open Data Institute[49] developed the following categories:

- **Closed Data** includes data that can only be accessed by its subject, owner or holder. For example, employee records.
- **Shared Data** can only be accessed by certain named people or organisations (medical research, for example); groups that meet certain criteria; or the public under certain terms and conditions. For example, twitter feed.

[45] *Id.*
[46] *Id.*
[47] Vargas, C. (2014). City settles gun permit posting suit. Retrieved 31 May 2020, from https://www.inquirer.com/philly/news/local/20140723_City_settles_gun_permit_suit_for__1_4_million.html.
[48] *Id.*
[49] Open Data Institute, "Open Data Institute," http://theodi.org.

- **Open Data** can be accessed, used and shared by anyone. For example, the bus timetable.

Citizens aren't very receptive to data release disclosures or privacy policies. Nissenbaum recommends that citizens should instead be empowered with "the right to control information about oneself."[50] Therefore, data releases must be accompanied with contextual details so that the public gains a comprehensive understanding of all the associated risks and benefits. This must clarify exactly what the data represents and its accuracy, and provide information about how it was generated.[51]

[C.1.3] Protection of Data

The challenge that arises with data protection is that the attempt to maintain privacy of individuals often comes at the cost of decreased utility of the data analysed. It is important to protect the privacy of individuals, while simultaneously ensuring that the trade off is not that of limiting research.

a. **Anonymous identifiers** can be used to protect the privacy of individuals. However, in order to be effective, the identifiers must be randomly generated i.e. having no connection to the attribute they replace. While anonymised data also faces the risk of re-identification, it would be safer to digitally encrypt the data collected.[52]
b. **Removing records** that contain sensitive data, either because of their easily identifiable features or because of the type of event represented. For example, removal of records of sexual assault from a dataset of police incidents would protect the privacy of those mentioned in the deleted records.[53] However, this would, only naturally, impact any analyses dependent on these records.

[50] Nissenbaum, H. (2004). A Contextual Approach to Privacy Online. *Washington Law Review*, *1*, 79. doi: 10.1162/daed_a_00113.
[51] *Supra* note 41.
[52] *Id.*
[53] *Id.*

c. **Re-identification testing** can be employed to deliberately expose the vulnerabilities in the data protection platforms, and then attempt to fix the problems exposed.[54]

d. **Regular auditing** is essential because, as mentioned earlier, that while data may remain the same, the risks are ever changing. The audit could examine the new forms of re-identification attacks, the shift in public perception with regards to data privacy, emergence of best practices etc.[55]

e. **Differential privacy** provides a mathematical guarantee of privacy against a wide range of privacy attacks, such as reconstruction or re-identification attacks. It also guarantees that the inference or analyses of data so protected will, in no way, be skewed by the lack of sensitive personal information being available to the researcher.[56] The Census Bureau in the United States, for example, classifies some of its data under the 'non-interactive' head, where data must be published or released before its use.[57] The reason differential privacy is being explored and developed on a large scale is that it protects against a wide range of attacks, including those that the developers may not have foreseen at the time of development. They also maintain transparency because the parameters and computation aren't necessarily a 'secret'.[58] It is also immune to post-processing, so a data analyst would not be able to compute the function of the output generated here to reduce its privacy protection, without a complete and comprehensive understanding of its private database.[59]

f. Additionally, in order to have a robust data protection framework, it is important to **clarify ownership of data** and assign the responsibility of data protection in order to increase accountability. Since Intellectual Property Rights (IPR) are difficult to assign due to the nature of data, clarity on property rights may help assist regulation. They

[54] *Id.*
[55] *Id.*
[56] *Id.*
[57] Gaboardi, M., Honaker, J., King, G., Murtagh, J., Nissimk, K., Ullman, J., & Vadhan, S. (2018). *PSI (Ψ): a Private data Sharing Interface*. Harvard. Retrieved from https://privacytools.seas.harvard.edu/files/privacytools/files/1609.04340.pdf.
[58] *Supra* note 41.
[59] Nguyen, A. (2019). Understanding Differential Privacy. Retrieved 31 May 2020, from https://towardsdatascience.com/understanding-differential-privacy-85ce191e198a.

would certainly increase transparency. Certification standards should be developed in order to maintain quality control over the data collected and analysed.

[C.2] Personal Data Protection Framework and the constitutional right to privacy

Though the personal data protection framework proposed by the MeitY through the Personal Data Protection Bill, 2019 is among the significant efforts undertaken by the Government in enabling an ecosystem to leverage digital platforms for governance, in its present form the framework is slightly lacking.

The interaction of the various systems involved in setting up open and secure digital delivery platforms with the data protection framework will be immense. The sheer volume of user data that will be required to be stored not only safely and securely, but also within the boundaries of the law. In light of the *Justice K.S Puttaswamy v. Union of India* judgement that cemented the right to privacy, it is imperative to look at any such framework in light of constitutional principles. Though the judgement specifically mentions that the right to privacy is not an absolute right and may be overridden by competing state and individual interests, it also specifies that such intrusions into the right must be subject to the satisfaction of certain tests and benchmarks.[60] The consultation paper released by the MeitY is lacking in this aspect, as it does not undertake an evaluation of the systems in light of these principles. Specifically, with respect to the proposed personal data protection framework, there are many aspects that require to be evaluated before any digital delivery platform at this scale is undertaken.

The collection, storage, processing and sharing of data under the proposed NODE will be undertaken at a large scale and on various. Thus, it is imperative that at each level there is maximum effort to undertake a consent-based approach with respect to the collection and processing of data, which are in consonance with international privacy principles. As per the

[60] Bhandari, V., Kak, A., Parsheera, S., & Rahman, F. (2017). *An Analysis of Puttaswamy: The Supreme Court's Privacy Verdict*. IndraStra Global, 11, 1-5. https://nbn-resolving.org/urn:nbn:de:0168-ssoar-54766-2

collection limitation principle of the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data[61] that there should be a *limitation on the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.* It implies that data is collected for a specified and limited purpose and with the due consent of an individual. To achieve such a system, it is necessary that certain standards are laid down that are to be adhered to by each component within this digital ecosystem. There is a need for uniformity in standards, as data is required to flow-freely between different actors for a variety of different purposes.

Though, the present version of the proposed data protection framework provides wide exemptions to the Government and Government authorized agencies[62] and provides them with leeway in maintaining such standards, it may not be the best way forward. It is important to create an environment of trust between the citizens and the Government when employing large scale digital delivery programmes that deal with personal data collection and processing. An ideal method of gaining the trust and cooperation of the public in executing such a system would be a robust privacy framework, that enables the individual to feel that their data is secure and that they have adequate redressal mechanisms in order to safeguard their data from misuse by any actor involved in the system. The absence of provisions relating to surveillance in the Personal Data Protection Bill, 2019 coupled with the exemptions granted to the Government also raise concerns regarding surveillance activities of the Government and misuse of the data that the Government is a custodian of. The Sri Krishna Committee had also raised concerns and the need for better legal provisions to govern surveillance activities[63], such recommendations must be taken seriously in light of such programmes to ensure that data collected for a particular purpose through a welfare programme is not misused, either by a Government agency or a private actor.

[61] OECD Council, (2013) , Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data , 14, http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

[62] Draft Personal Data Protection Bill, 2019, Ministry of Electronics and Information Technology, Section 35, https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf

[63] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (2018), Page 124

Examples of such breaches have occurred in the past, wherein due to lack of clarity with respect to privacy design or protocols, Government initiatives have come under the scanner for having a lax approach to data privacy. The "Vahan", a digitized vehicle register, created by the Transport Ministry, raised privacy concerns as it was brought to the public's notice that the Ministry was providing access to data collected by the App to government and private entities on a payment basis,[64] however it also came to light that unscrupulous third-party apps also had access to the data bases illegally.

Secondly, by undertaking such an ambitious digital delivery in light of the data localization requirements placed by the Personal Data Protection Bill, 2019[65], where in certain categories of personal data such as critical personal data can be processed only within the territory of India, bring to light questions about India's data storage and processing capacity. The Indian data center market is currently operating at a capacity of approximately 700 MW, which caters to data generated by 493 million active internet users, which pales in comparison to Europe's data center capacity of more than 8600 MW with 460 million internet users.[66] In absence of a concrete plan envisioned by the Government to ramp up its data storage capacity, and providing incentives that create a lucrative market for data center providers, it is possible that India's plans to transition into adoption of GovTech 3.0 may lack the requisite technical backing.

[64] The New Indian Express, "*SARATHI, VAHAN data earned Rs 65 crore* https://www.newindianexpress.com/states/tamil-nadu/2019/jul/14/sarathi-vahan-data-earned-rs-65-crore-nitin-gadkari-2003595.html

[65] Draft Personal Data Protection Bill, 2019, Ministry of Electronics and Information Technology, Section 33- 34, https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf

[66] Gupta, Sunil, *India may have 800 million internet users by 2023 if it can get this factor right,* 2020, Financial Express, https://www.financialexpress.com/industry/technology/india-may-have-800-million-internet-users-by-2023-if-it-can-get-this-factor-right/1816771/,

[C.3] IPR and Competition

Data itself has very little value. According to Catrona Maccallum, an Advocacy Director at PLOS, it's value becomes apparent only when it is Findable, Accessible, Interoperable and Re-usable.[67] However, forms of metadata can receive copyright protection. For example, graphs, charts and other forms of visualisations would satisfy the Supreme court requirement of 'modicum of creativity'.[68] The Court of Justice of the European Union provides a *sui generis* right to databases[69] that require investments in obtaining the data and not the creation of the underlying data. The exception to this right is non-commercial research. This is problematic for several reasons, not the least of which is the clear pathway for a monopolistic market.

It's clear that with the establishment of NODEs, there will be immense growth in the 'data collection market' with companies like Facebook, Amazon and Google having distinctive advantages. Smaller companies would have to develop machine-learning algorithms and cloud computing services in order to be able to begin data processing on a large scale.[70] The market created would have large revenue opportunities because there will be significant developments in the technology sector as well as the data analytics sector. However, the larger players would exclude their inclusion within the market, so there is reduced consumer choice, predatory pricing and ultimately limited innovation.Competition law principles like "abuse of dominance" would help reduce the number of such occurrences. For example, in the *Magill* case, the BBC and others attempted to create a secondary market. Their primary function was to distribute and

[67] Crouzier, T. (2017). *IPR, Technology Transfer & Open Science*. European Commission. Retrieved from https://publications.jrc.ec.europa.eu/repository/bitstream/JRC106998/kj1a28661enn.pdf.
[68] Eastern Book Company v. D.B.Modak, 1 SCC 1 (Supreme Court of India 2008).
[69] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases.
[70] Lundqvist, B. (2016). Big Data, Open Data, Privacy Regulations, Intellectual Property and Competition Law in an Internet of Things World. *Stockholm Faculty Of Law Research Paper Series*.

produce TV shows, and they thus created TV listings, which would be copyright protected. The secondary market would've been based on the sale of these TV listings.[71]

Regulatory guidelines must therefore ensure minimal entry barriers within the market, ensure the IPR is owned by the government, at least in the initial stages of development, and must be monitored closely. In Kenya, for example, the rise of digital lending has raised the risk of over-indebtedness.[72] Additionally, the World Bank's Consultative Group to Assist the Poor (CGAP) observed that at least one digital credit product within that market resembles a ponzi scheme.[73] The regulatory sandbox created via the Personal Data Protection Bill, 2019 will play a very important role in this regard. While the bill creates high compliance costs for small businesses, the regulatory sandbox, if expanded to be more inclusive, could offer some form of respite. For example, Maharashtra is looking to create a regulatory sandbox for the employment of blockchain technology for e-governance.[74]

The best way to strike a balance between innovation and traditional profit motives, is to develop a licensing regime. While the revenue opportunities themselves create incentives for innovation, licenses allow access to data that would otherwise be too expensive to access and would inevitably create friction.[75] Licensing regimes, such as compulsory licensing, also limit the entry barriers for smaller businesses. For example, several organisations have signed the Open COVID pledge which allows access to intellectual property rights (except trademarks and trade secrets) to use, share, copy, distribute etc. until a year after the World Health Organisation (WHO)

[71] *Id.*

[72] Izaguirre, J., Kaffenberger, M., & Mazer, R. (2018). It's Time to Slow Digital Credit's Growth in East Africa. Retrieved 31 May 2020, from https://www.cgap.org/blog/its-time-slow-digital-credits-growth-east-africa.

[73] di Castri, S., & Plaitakis, A. (2018). *Getting Financial Inclusion Policies Right in the Digital Era: Focus on Competition and Innovation as Policy Objectives*. Centre for Financial Inclusion.

[74] Bhalla, K., Bhalla, K., & Staff, I. (2020). Maharashtra Launches Blockchain Sandbox For E-Governance. Retrieved 31 May 2020, from https://inc42.com/buzz/maharashtra-launches-blockchain-sandbox-for-e-governance/.

[75] Agrawal, A. (2020). #NAMA: Considering intellectual property rights over non-personal data. Retrieved 31 May 2020, from https://www.medianama.com/2020/01/223-intellectual-property-rights-non-personal-data/.

declares the pandemic to have ended. However, certain licenses under this pledge only allow access to copyrights, while some only extend this right to January 2023.[76]

For example, a Business Source License (BSL) gives the licensee complete access to the source code, so the licensee can modify, distribute and enhance it. Only when the licensee uses more than *x* amount of code, the licensee must pay a certain fee. A contributor license agreement on the other hand, allows open source projects to re-license their products if/when a better license arrives. This allows the developers to ensure some sort of protection in case of future developments.[77]

[76] Open Covid Pledge. (2020). Retrieved 31 May 2020, from https://opencovidpledge.org/.

[77] Buytaert, D. (2019). 3 suggestions for stronger open source projects. Retrieved 31 May 2020, from https://www.infoworld.com/article/3451778/3-suggestions-for-stronger-open-source-projects.html.

5. Community

At the heart of every governance system lies the involvement and inclusion of the community. This aspect has been highlighted in the principles listed in the consultation paper released by the MeitY[78] namely ensuring inclusiveness, facilitating participatory design, driving user engagement and enabling grievance redressal mechanisms. These principles encompass the true aim of any such project that is to provide seamless governance models, for both the Government to utilize and for the citizens to access and use. The participatory design aspect is an attempt to ensure that such a system created is a result of collaborative effort between the society and the Government, which facilitates innovation and development.

Ensuring inclusiveness may prove to be a large challenge for India's aims of creating open and secure digital delivery platforms. As India has a very diverse demographic profile, it is imperative that every section of society has universal and affordable access. The Government must strive to ensure that systems must be accessible to each citizen and also ensure that digital awareness and literacy is promoted at all levels of society. Prior to undertaking any major paradigm shift,

Though creating requisite technical capacity and ensuring last mile connectivity are major challenges to be conquered in the Indian context, a major issue often ignored, is that of promoting digital literacy and awareness to end-users on how to utilise e-governance platforms or services. Digital literacy according to the Digital Literacy Global Framework developed by UNESCO is the "*ability to access, manage, understand, integrate, communicate, evaluate and create information safely and appropriately through digital technologies for employment, decent jobs and entrepreneurship.*[79] As per the framework, it includes competences that are variously

[78] *Supra* note 1.

[79] Law, N. W. Y., Woo, D. J., de la Torre, J., & Wong, K. W. G. (2018). A Global Framework of Reference on Digital Literacy Skills for Indicator 4.4. 2

referred to as computer literacy, ICT literacy, information literacy and media literacy.[80] These are the nuances that highlight the “digital divide” rather than the access to technology per se. It is imperative that while understanding this we acknowledge all forms of digital inequality - such as

1. Hardware, Software and Connectivity
2. Freedoms of use and access
3. Harmonisation of use patterns
4. Skills and ability to use the internet effectively
5. Support networks and troubleshooting assistance

Inadequate technical means is India’s largest hurdle in implementing programmes along the lines of the NODE. Such is evidenced by low internet penetration in India and access to inadequate technical means in rural communities, who are largely the focus of welfare programmes. According the a report by the IAMAI on internet usage in India[81], that the penetration of internet in urban India (with a base of 192 million users) is twice that of rural india. The report also highlighted how, though there may not be a large gap in terms of absolute number of internet users in urban and rural areas, there is enough headroom for growth as 70% of the rural population does not access the internet actively.[82] Such factors will play a huge role in ensuring smooth functioning of systems, as it requires users to have seamless access to components that require internet connectivity. At present, though we have high speed internet in certain urban areas, many rural communities struggle to have access to stable mobile connectivity. Though efforts of the government to mitigate this issue are ongoing, not many tangible results are being seen. For example, the Government has implemented flagship schemes like Bharat Net Project,

[80] *Ibid.*
[81] IAMAI, & Nielsen. (2019). *India Internet 2019*. Retrieved from https://cms.iamai.in/Content/ResearchPapers/d3654bcc-002f-4fc7-ab39-e1fbeb00005d.pdf
[82] *Ibid.*

but according to the latest internal government data, fewer than 2.5% of India’s 2.5 lakh village panchayats have commercial broadband connections.[83]

However, the availability of digital resources is not the sole hurdle in the Indian context, economic and social disparities also lead to constraints on usage. Between 2014 and 2017, there was a 26 per cent increase in the affordability of mobile internet—the largest increase among all countries assessed in the Mobile Connectivity Index during this period.[84] Concerns of affordability aside, India is home to unique problems such limited access and gender gaps in mobile phone usage[85]. These concerns largely impact ensuring complete inclusiveness of any system thus created digitally. Along with the promotion of penetration and technical capacity, it is recommended that the Government keep in mind promoting holistic digital literacy as a part of formal education imparted.

The principle of inclusiveness works inconsonance with that of participatory design, and fosters representation. By involving actors from within the community to participate in the process of building systems and technologies, we may be able to address the more nuanced issues present in the Indian context.

An important aspect of engagement with a community is providing them with an adequate avenue of grievance redressal, it helps both in quick resolution of issues but also helps build an atmosphere of trust. The ambitious nature of NODE, and the numerous systems that will work in collaboration to deliver services highlights a need for a clear grievance redressal mechanism at each varying level. It is suggested that rather than relying entirely on legally mandated grievance

[83] Gairola, M. (2018, November 2019). In ‘Digital India’, Not Even 2.5% Panchayats Have Commercial Broadband. The Wire.
[84] State of Mobile Connectivity, 2018, GSMA, https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2018/09/State-of-Mobile-Internet-Connectivity-2018.pdf
[85] The Mobile Gender Gap Report, 2019, GSMA https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/02/GSMA-The-Mobile-Gender-Gap-Report-2019.pdf

redressal models, different organisations also internalize easy grievance redressal mechanisms. If at each level the individual is provided with dedicated mechanisms to deal with issues along the lines of specific helplines for technical assistance and those for user complaints for example, we may be able to make the system more seamless and user friendly. With respect to legal complaints, it would be helpful to create easy to access and understand forms for users so that data may be collected in a standardized manner to ensure ease of administrative processes at a later stage.

Recommendations:

1. The Dialogue recommends that the platforms and systems formulated as a part of this programme are multilingual, more graphic and less text-based.
2. The Dialogue recommends that platforms must not be overly reliant on literacy and digital literacy at the outset to promote universal access and inclusiveness.
3. The Dialogue recommends varied representation at various levels to ensure that the interests and sensitivities of all vulnerable sections of societies are addressed.
4. The Dialogue recommends that the Government undertake structural changes in the ICT and Computer Science curriculum from primary and secondary levels to include modules that promote digital literacy with respect to data rights, online safety and privacy in addition to a technical education pertaining to these fields.
5. Enable grievance redressal mechanisms to function both internally within organisations through standard operating procedures for all organisations involved and through regular legally mandated grievance redressal systems.

[A] Question 8:

What are effective means to mobilize the wider community and build a vibrant network of co-creators who can develop innovative solutions on top of open platforms? What can we learn from other platforms or sectors?

In our research we have come across two prior government engagements that have been successful in achieving greater onboarding, and participatory design. DPIIT tied with Startup India during the COVID-19 pandemic to innovative technologies and solutions for precautionary and treatment-related interventions. This has led to greater participation in the design of solutions that fit the criterion and incentivises the community to solve problems and challenges together. Similarly in a historic move, Aarogya Setu was open sourced with the intention of collaborating to build a more robust app. This is an example that can be looked at for examples in the recent past that have received widespread response.

[B] Question 9:

Are you aware of any end-user adoption and engagement models that platforms have successfully adopted e.g. feedback loops, crowdsourcing use cases, offline awareness and on-boarding campaigns?

An effective grievance redressal model will foster greater public trust. This will allow for more user adoption. A clearer regulatory landscape will also allow for more user engagement. Digital India Programme has also proposed using satellites, balloons, or drones to bring faster digital connections to remote parts of the country. [86]

[C] Question 10:

Are you aware of any innovative grievance redressal mechanisms/models that go beyond customer support helplines to augment accountability to citizens? If yes, please describe along with examples.

Please refer to section 1 [H] - Principle 15.

[86] Centre ready to use satellites, drones to connect to rural India: Ravi Shankar Prasad. (2020). Retrieved 31 May 2020, from https://economictimes.indiatimes.com/industry/telecom/centre-ready-to-use-satellites-drones-to-connect-to-rural-india-ravi-shankar-prasad/articleshow/46115684.cms

6. On Support Required

A. Question 12: What kind of tools (e.g., case studies, workshops, online knowledge banks, access to experts, etc.) would be most useful for your organization/ department to enable you to take this approach forward?

As a technology policy think tank, we would recommend that the public outreach programme under NODE should be transparent and accountable. After the completion of the present round of public comments, MeITY should come up with a detailed white paper addressing the solutions and concerns based on the recommendation received and invite a round of public consultation again. Further, individual consultations based on the revised white paper should be done with different organisations that are concerned with the matter at hand.

B. Question 13: How would you like to engage further (e.g. individual consultations, workshops, etc.) as we build the strategy for NODE?

As a research and advocacy organisation having expertise in the technology policy issues, we could support this projects on two fronts i.e. Research and Engagement. We can assist the ministry and the concerned department with the relevant research and developing solutions to the different issues involved. Further, the Dialogue can also assist with wider stakeholder engagement for the Meity to obtain varied suggestions from developers, academicians, end users etc.

7. About The Dialogue

The Dialogue is an emerging public-policy think-tank with a vision to drive a progressive narrative in India's policy discourse. Founded in 2017, we believe in facilitating well-researched policy debates at various levels to help develop a more informed citizenry, on areas around technology and development issues.

Our aim is to enable a more coherent policy discourse in India backed by evidence and layered with the passion to transform India's growth, to help inform on public-policies, analyse the impact of governance and subsequently, develop robust solutions to tackle our challenges and capitalise on our opportunities. To achieve our objectives, we deploy a multi-stakeholder approach and work with Government, academia, civil-society, industry and other important stakeholders.

Contact Details:

Kazim Rizvi, Founding Director

Kazim.r@rthedialogue.co