Comments on the ‘Strategy for National Open Digital Ecosystems (NODE)’ Consultation Whitepaper

Rishab Bailey, Harleen Kaur, Faiza Rahman and Renuka Sane

National Institute of Public Finance & Policy (NIPFP)*

May 31, 2020

Contents

*Rishab Bailey, Harleen Kaur, Faiza Rahman are fellows at NIPFP. Renuka Sane is associate professor at NIPFP. The views expressed are personal. The authors would like to thank Professor Ajay Shah, Smriti Parsheera, Pratik Datta and Sarang Mohrir for their valuable inputs.

1 Introduction

The Consultation White-paper (CW) envisages a NODE as a platform that will enable the opening up/sharing of personal and non-personal data held in a particular sector (largely by government agencies), thereby enabling the development and provision of innovative solutions to individuals. If required, new institutional mechanisms will be created to oversee and govern such platforms.

Such an initiative is seen as enabling: (a) greater intra-government and public-private coordination, (b) the institution of robust governance processes, (c) the private sector to build services on newly opened-up data sets, thereby promoting innovation and efficiencies and enhancing citizen's ability to access (e-governance and other) services. The summary of our comments is as follows:

1. Building a platform or mandating the use of specific technological solutions is not a core function of government. The market failures identified in the CW such as lack of trust may be solved through certification standards without the government building and operating the infrastructure. There is a need to do a root cause analysis of the frictions in each sector to identify the least intrusive way of solving the same. These principles are discussed in detail in section 2 under *Limited state intervention* and *Role of the State.*

2. The government should focus on opening up appropriately identified datasets to the public, in a non-discriminatory manner. The government should not seek to build, operate or mandate the use of specific technological architectures, except as may be needed for its core functions. All government technology must, as a preference, be based on open standards, open source software and open APIs. These principles are discussed in section 2 under *Limited State intervention*, and *The role of the State* and in section 3, under the discussion on the principle titled *Open and Interoperable.*

3. In establishing / operating / regulating any digital infrastructure, the government must adhere to principles of accountability, transparency and openness, and ensure that all fundamental rights are adequately protected. The principles are discussed in section 3, specifically under the discussion on principles *Open and Interoperable* and *Privacy and Security.*

4. In its role as a regulator of the digital infrastructure owned and operated by the private sector, the State must ensure maintenance of a competitive environment, and appropriate governance frameworks that constrain egregious behaviour by private entities. These principles are discussed in detail under section 5.

In this document we describe our governing principles and respond to the questions laid out by the CW.

2 Our governing principles

The government plays an important role in providing public goods (such as police, courts, defense, etc.), providing welfare or other state services (such as the Public Distribution System (PDS), MNREGA, licensing etc.), and creating conditions to solve for market failure through regulation. Our view is that *building* a platform or mandating the use of specific technological solutions is not a core function of government. Excessive government intervention may increase the chances of the single sources of truth turning into single sources of failure and decrease innovation and competition. The government is also not suited to keeping pace with the speed of technological development. Any over-regulation or excessive centralisation could have negative effects on expected outcomes. The government should, therefore, create the rules of the game so as to harness the innovation that a competitive environment can bring while ensuring appropriate standards of governance and fair-play. Our governing principles are as follows:

1. *Limited state intervention:* The state must, as a general rule, only be involved with building technological infrastructure only in case of essential state activities, including in relation to its welfare functions.

   There is a need to differentiate sectors where the state has a legitimate role (say in the provision of its welfare and statutory functions), from sectors where private sector solutions could suffice. That is, the state should have a role in providing access to PDS, but need not be a player in building a platform for access to rail reservations. Therefore, one must ensure clear evidence of the need for state intervention in creating any digital infrastructure.

   For instance, the CW identifies the market failure in the skills sector to be twofold, (i) information asymmetry amongst the stakeholders and (ii) a lack of trust in the information that is available. Thereafter it goes on to propose the Talent (Skilling and Job) Node as a one stop portal which connects employers, job seekers, counsellors and skilling institutes. It is recommended that before implementing the Talent NODE, the government should enquire if private entities can or are already innovating to bridge the information asymmetry and trust issues in the sector. For example, at present the skills sector is already being served by government portals[1]

[1] See National Career Service portal(https://www.ncs.gov.in) and bharatskills.gov.in

and private service providers such as https://www.leapskills.in, www.babajob.com, urbanclap.com and https://www.skillr.ai.

If the problem in the skills sector is a lack of trust, this can be solved by interventions such as certification standards. The solution to information asymmetry does not necessarily lie in the government providing the service. Therefore, before the Government creates infrastructure for a Talent Node that connects various stakeholders in the skills sector, it is critical for the government to establish why incentivising private sector innovation by providing open APIs will not address the market failure. The government also needs to evaluate why the private sector would voluntarily come onboard an infrastructure developed by the government.

Consequently, putting in place appropriate regulatory structures should be the primary focus of the state in so far as the second set of (private sector based) solutions is concerned. Such a differentiation would promote innovation, prevent the emergence of a state centric technological monoculture and allow the private sector to respond appropriately to requirements of any particular sector (as opposed to being forced to build on top of state mandated infrastructure, which may not always be necessary or appropriate in a particular context).

2. *Avoid creating monolithic, centralised platforms:* Any platforms made by the public sector must allow for federated and decentralised systems as far as possible. The creation of monolithic technical architectures (which are often de facto mandatory) must be avoided. For instance, the creation of a centralised identification system (Aadhaar), which is then mandated for use across different sectors has lead to various problems ranging from exclusions and excessive intrusions on privacy, to limited innovation (i.e. such a system is preferred over other possible forms of identification that could suffice in any particular use-case). Technology moves too fast and has multiple possible future use cases. Implementing a centralised system of 'public infrastructure' may therefore not be necessary in multiple sectors, where the focus should be on enabling the private sector to develop relevant platforms and technologies that compete with one another (with due consideration for regulatory, human rights and other problems that may arise in any given context).

3. *The role of the state*: The state should build platforms/digital infrastructure, only where required due to its governance/constitutional/statutory mandates, say in the context of taxation, PDS, access to licensing systems, etc. The role of the government should primarily be to (a) identify appropriate sectors and data sets to open up, (b) standardise record-keeping formats

and build relevant databases, (c) ensure appropriate governance frameworks, which may relate to for instance, protecting civil liberties, competition regulation, etc.

3 Response on the guiding principles set out in the CW

Question 1: Please comment on the guiding principles defined in Section 4 and indicate whether there are any principles you would add/amend/drop. Please provide reasons for the same.

Our comments on the guiding principles are as follows:

1. *Open and Interoperable:* Any interventions by the State must, generally speaking, be technology neutral and avoid over-prescription. The government should not be in the business of 'picking winners', enabling enrichment of certain interests at the cost of others or creating technological monopolies. Participation and market competition should be promoted.

   We broadly agree with the principle of open and interoperable delivery platforms. However, the scope of such "openness" must be clarified.[2]

   Instead of redefining "openness" as is sought to be done in the CW, the definition must be consistent with and build on existing definitions[3] and

[2] The current definition of openness in the CW is: *"the term "open" in NODE refers to principles of openness, including but not limited to transparency, accessibility, inter- operability, open APIs and standards and open source code, where appropriate. However, it must be noted that each NODE will have its own configuration and degree of "openness", which may introduce certain limitations in order to adhere to specific objectives, context or to mitigate potential risks."*

[3] We note that the Government of India's existing policy on Adoption of Open Source Software defines "Open Source" as referring to the availability of source code for the community / adopter / end-user to study and modify the software and to redistribute copies of either the original or modified software (without having to pay royalties to previous developers). Further, the Framework for Adoption of Open Source Software in e-Governance Systems, notes with approval the definitions of the term used by the Free Software Foundation and Open Source Initiative. Accordingly, open source should not mean merely providing access to the relevant source-code, but also (a) ensuring free redistribution, (b) allowing distribution of transparent source code, (c) permitting derivative works to be made, (d) non discrimination, (e) technology neutral, (f) licensing must not be specific to a product or restrict usage of other software, (g) rights attached to the code must apply downstream without further licensing requirements etc. (The Open Source Initiative, 2017)

government policies pertaining to the use of open source software solutions, and open APIs.[4]

We note in particular that:

- one of the objectives of the National Policy on Information Technology, 2012, (NPIT) is for the Government adopt open standards and promote open technologies. The NPIT also requires the adoption of open standards and technologies in e-Governance projects.
- the Policy on Adoption of Open Source Software for Government of India requires the government to give preference to open source software solutions in any e-government projects.
- the Policy on Open Standards for e-Governance aims to facilitate interoperability between e-Governance systems, and mandates that the Government shall adopt single and royalty free open standards progressively for specific purposes within a domain.[5]
- the Policy on Open Application Programming Interfaces (APIs) for Government of India mandates the adoption of Open APIs in e-Government applications and systems.[6]
- the Framework for Adoption of Open Source Software in e-Governance Systems, 2015, provides guidance to governments and agencies in promoting, managing and adopting OSS as a preferred option in e-Governance systems.

The above policies pertaining to openness of software used in e-Governance platforms must be retained / strengthened / implemented in the NODEs

[4] An indicative list of such policies include the Policy on Adoption of Open Source Software for Government of India (as well as relevant state and departmental level policies), Framework for Adoption of OSS in e-Governance Systems, 2015, Policy on APIs for Government of India, 2015, Policy on Open Standards for e-Governance, Interoperability Framework for e-Governance, 2015, Policy on Collaborative Application Development by Opening the Source Code of Government Applications, 2015, Implementation Guidelines for Open API Policy for e-Governance, 2020, etc.

[5] The document also lays out the mandatory and desirable characteristics for qualification of a standard as an 'open standard'. Alternate standards are to be adopted only in case standards with the mandatory characteristics are not available.

[6] Importantly, information provided through the APIs should be open and machine readable; all relevant information and functionalities of an e-Governance system are to be made available to other e-Governance systems, through platform and language agnostic Open APIs; Government organisations consuming data form others are responsible for undertaking authentication and authorisation processes; every API is to be properly documented with the sample code and sufficient information published so as to enable developers to make use of the API.

projects.[7]

These should be applicable to both government and private entities participating in NODEs, while providing for reasonable exceptions. For instance, interoperability can be achieved through data standardisation which can be made mandatory for participation in a stack. For instance, the Electronic Health Records Standards 2016 are notified and have to be followed by both government and private players for interoperability.[8] Open APIs and open standards should be mandatory for private entities whenever the entities have a role in governance and/or utilise pubic goods shared by the government in the NODEs. The openness and interoperability standards will depend on the nature of the stack and should be built upon existing government policies, if required.

Openness must apply to the standards used to build tools/APIs used in any project, as well as the non-discriminatory nature of access to relevant data sets.[9] This would ensure (a) the benefits of open source software and APIs are realised in any public sector interventions (such as enhanced security, no vendor lock-in etc.), (b) multiple parties can build solutions on top of government data, and therefore compete to both build infrastructure and provide relevant services to citizens.

For example, the benefits of opening up railways related data, subject to relevant norms pertaining to personal data, (currently monopolised by IRCTC) can enable the provision of customised/personalised travel solutions to consumers. Greater linkages could be formed with private players in the hospitality and travel/tourism sectors leading to mutual benefits to the railways as well as the private sector and consumers.

2. *Ensure security and privacy:* Ensuring appropriate data security/privacy will be one of the primary challenges of a NODEs ecosystem, particularly given current levels of technical expertise and education in India.[10] Building

[7] Using proprietary code to deliver public functions/infrastructure could lead to inequitable and anti-competitive outcomes, in addition to perpetuating well-recognised problems with proprietary software (such as security concerns, vendor lock-in, high licensing and replacement costs, etc.). Notably, the Framework for Adoption of Open Source Software in e-Governance Systems, 2015 lists numerous benefits of the use of OSS.

[8] See, Ministry of Health and Family Welfare, 2016.

[9] Without derogating from the need for relevant access control and other mechanisms to be implemented, as may be required in specific instances.

[10] A breach of privacy of NODE data can result in harms suffered by individuals and/or communities. For instance, news reports allegedly that government data on vehicle registration, publicly accessible via the mParivahan app, was used to target cars belonging to members of a minority community during Delhi riots in February 2020 (Chunduri, 2020).

capacities in terms of adequate institutional, legal and technical expertise will be essential. Engagement with the private sector and broader citizenry will be vital in this process.

Relevant authorities/government institutions will need to ensure that data sets are appropriately tagged for public use, and that any downstream risks are minimised. As recognised in the CW, ensuring privacy by design - i.e. considering the risk involved in every stage of the data flow / lifecycle of data will be important prior to opening this up for use. Appropriate frameworks for data breach notification, security protocols etc., will also need to be implemented on a sectoral basis.

One may consider implementing frameworks based on appropriate fiduciary principles, thereby assigning responsibility to entities dealing with citizen data. These should go beyond the mere use of 'fiduciary' terminology, to ensure that data collected by the government is actually used in a citizen's best interest / for her benefit. Appropriate standards of duties of care and loyalty could be imposed, that, where necessary, go beyond the obligations imposed under the draft Personal Data Protection Bill, 2019.[11] This may take the form of for example, creating multi-stakeholder data trusts or other similar systems to ensure adequate data protection and fair value exchange.

Where personal data is concerned, citizens must have the ability to make granular and informed choices regarding what uses their data is put to. The issue of obtaining granular consent becomes even more important if personal data is shared across NODEs, as indicated by the CW. As an example, Estonia's smart government seeks to obtain granular consent from its citizens by not maintaining a centralised database, and storing the data about taxes, education, healthcare etc. in separate databases. Further, the citizens are also able to decide which entity gets to see what information. For instance, an Estonian citizen is able to decide if their cardiologist can share their data with their neurologist.[12]

We would also caution against the wholesale adoption of untested and possibly inadequate systems such as consent aggregator frameworks as a panacea for all consent related issues.[13] Instead, it is suggested that the multiple technical systems should be allowed to operate in the consent domain as well that compete for providing the best solutions to ensure that free, informed, and granular consent is obtained.

[11] (Bailey and Goyal, 2019) and (Bailey and Goyal, 2020).

[12] Barlow and Levy-Bencheton, 2018.

[13] Malavika Raghavan and Anubhutie Singh, 2020.

We believe that an enforceable legal framework requiring government and private parties to ensure privacy and security should be implemented as a pre-condition for initiation of NODEs in any specific domain. While certain steps have been made in this direction - for example, the NDHB proposes a National Policy on Security of Health Systems and Privacy of Personal Health Records for its stakeholders[14], we believe that such policies should be converted into enforceable law as has been done in other jurisdictions.[15] The proposed law should take into consideration general privacy principles and the specific nature of data and its intended use in the particular domain.

Finally, it will also be relevant to ensure consistency with legal and policy frameworks created under the draft Personal Data Protection Bill, 2019, as well as in terms of the Recommendations of the Expert Committee on Data Governance Framework headed by Kris Gopalakrishna.

3. *Agile, data driven development method:* While in general, an agile and iterative method for building technical solutions may be important, this should not take away from the need to think through the possible impacts and pitfalls that may arise in any particular sector. An excessively 'iterative' way of development may lead to (a) slow uptake of systems due to real or perceived problems with a platform, (b) erode public trust in a platform if unable to carry out key functions, (c) may devolve into a system of applying 'bandaid' solutions to systemic flaws. A certain degree of planning may therefore be required, particularly where public service delivery is concerned. Appropriate testing must also be built into roll-out plans, to ensure systems can function appropriately and that any unintended outcomes (such as exclusions) are limited. For instance, Michaelson, 2017 studied the adoption and usage of Agile methods by the UK government for its Universal credit scheme. By studying policy and consultation documents, the author highlights the issues of scalability, exclusion and persistent structural problems such as inability to concomitantly adopt departmental procurement, policy development and operational management for the scheme.[16]

4. *Accountable institutions:* Delineating accountability of any project will be essential in ensuring appropriate regulatory outcomes, protecting citizens rights and ensuring a level playing field in each sector. It may be necessary to implement different institutional mechanisms for different sectors and it is premature to decide which mechanism is required in any particular sector.

[14] See, Ministry of Health and Family Welfare, 2019, at pg. 10.

[15] For example, *Health Information Technology for Economic and Clinical Health Act*, 2009 (US) and *Personally Controlled Electronic Health Records Act*, 2012 (Australia).

[16] See, Michaelson, 2017.

That said, principles of open, transparent and participatory governance, and appropriately democratic accountability frameworks must always be maintained.

In particular, it may be important to consider building mechanisms to ensure:

(a) *Participatory governance*: Participatory governance should form an integral part of the NODEs project. Democratic accountability of regulatory institutions must be maintained. This is particularly important should any governance structures be privatised. For example, the National Payments Corporation of India (NPCI) functions as a quasi-regulatory agency due to the scope of its powers/functions and de-facto regulatory monopoly. However, it does not come under the purview of the Right to Information Act being a private entity. This limits the ability of stakeholders to engage or for citizen centric governance to take place.

(b) *Co-ordination between different agencies*: It will be essential to put in place frameworks to enable allocation of responsibilities and coordination between government entities at different levels (local, state and central), when dealing with common issues (such as tagging of data sets, ensuring data quality, instituting grievance redress mechanisms, etc.), without usurping constitutional and statutory functions.

For instance, the skills sector is currently overseen by a number of government bodies both at the central and state level. While the Ministry of Skills and Development is the overall coordination body regarding skill development efforts across the country, the National Council for Vocational Education and Training (NCVET) will regulate vocational education and training institutes and establish standards for their functioning, the Ministry of Human Resource Development is responsible for governing polytechnics and apprenticeships for graduates, technicians, vocational technicians,[17] and Ministry of Rural Development has instituted skilling and placement initiatives for rural youth.[18] Apart from this, state level department of technical education, training and skill development [19] and State Council for Vocational Level (SCVT) also exist. Such a fragmented regulatory ecosystem will require a significant amount of coordination between multiple ministries and departments

[17] FICCI and KPMG, 2014.

[18] See Ajeevika Skills guidelines (Ministry of Rural Development, 2013)

[19] As an example, see the Department of Technical Education, Training and Skill Development set up by Government Of West Bengal which supervises polytechnics and vocational training institutes, and coordinate all skilling intervention (West Bengal, 2019).

at state, central and local levels.

Clarity of purpose and functions of various regulatory authorities involved in the stack would be necessary for NODEs to achieve accountability. As suggested earlier, one of the ways in which valuable synergies can be drawn through cooperation between multiple regulators is by requiring them to enter into a Memorandum of Understanding (MoU) for the coordination of their activities. In addition, any regulatory framework mandating such MOUs should also lay down a non-exhaustive list of provisions that need to be covered in the MoU to ensure clarity of purpose and better coordination.[20]

5. *Rules of engagement:* Rules of engagement in each sector must be clearly defined and consistent.

   Putting in place appropriately open, transparent and participatory processes for decision/rule making will be vital. In particular, care must be taken to ensure that vulnerable sections of society, and other stakeholders who may not typically be able to engage with such processes are included.

   In general, the state must avoid excessive intervention in terms of either creating platforms/technical solutions, where not strictly required or in mandating the use of any technical infrastructure/solutions.[21]

   Regulatory interventions must aim to (a) promote effective competition in each sector and maintenance of a level playing field, (b) avoid function creep and problems associated therewith, (c) consider the effect of any platform on the promotion and protection of fundamental rights, (d) ensure appropriate apportioning of functions, obligations and responsibilities/liabilities arising therefrom.

   In projects that are not linked to essential state functions, interventions must be based on a defined regulatory need (such as the need to protect privacy rights, promote competition, etc.) In general, regulatory interventions in the private sector must be considered only in the case of identified market failures.

   Care must also be taken to ensure that conflicts of interest are minimised (say in terms of the government recruiting private sector players to build/operate systems) who are also market players or otherwise have vested interests in development of service delivery solutions.

[20] Bailey et al., 2020a.

[21] In particular, the state must avoid mandating the use of any digital solutions in order to access state services.

6. *Transparent data governance:*

   Each sector will need to have its own data access and sharing policies (including in sofar as sharing of private sector data is concerned, say in the context of data gleaned from IoT devices installed in public spaces by private companies). In addition to well recognised principles such as data minimisation, limiting data collection, purpose limitation, etc., one may specifically need to consider:

   - how to regulate permissible downstream uses of data and avoid recombination of anonymised data sets to reveal personal data,
   - how to implement appropriate methods of control over data flows, without always resorting to excessively intrusive methods such as large scale data localisation,
   - how to implement appropriate systems to ensure auditing of platforms,
   - how to account for competition related issues arising out of structural problems in the digital economy, not least given the presence of network effects and the economies of scale in the data processing/AI sectors.[22]
   - how to ensure governance mechanisms are inclusive and participatory.

   For example, in the health domain, there are two broad types of digital databases envisaged in NDHB. These are, a) information about healthcare providers -a directory of hospitals, doctors, nurses etc., and b) Electronic Health Records -longitudinal records of a person (EHR). The data access and sharing policies for these would have to be developed as per their classification. For instance, the directory database of healthcare providers is a public good can be made shareable without any privacy concerns, but this data would be time sensitive. On the other hand, EHR data governance would need stricter protocols. Mere use of technology such as anonymisation and consent tracker without clarity of governance principles such as ownership of data and purpose limitation would not be sufficient to determine data access and sharing policies.

7. *Right capabilities:* As discussed previously, we do not believe that the state should be involved in building or operating platforms, except when it comes to essential state functions.

   That said, building appropriate capacities within the government to run such

[22] This may require re-evaluating existing competition law principles and their application to the data economy or recognising economic rights associated with both personal and non-personal data, etc.

projects, and ensure appropriate regulation of private sector led projects will be essential. Education and awareness, skilling will therefore be essential components. Given the broad scope of some of the NODEs projects, it will be essential to build capacities at local levels of governance. This will also enable greater buy-in by bureaucrats and other government functionaries who may be reliant on legacy systems.

The overarching regulatory system must recognise the need to implement appropriate guidelines/processes for tagging/publishing relevant data sets, methods to minimise downstream harms or minimise risks, etc.

8. *Suitable financing model:* Before initialising a NODE, the responsible ministry should analyse if the NODE is serving a welfare other essential function of the government. In case there is no element of welfare, etc., the government should not use its finances on creating infrastructure for such a NODE. For other cases, government participation should be limited to serve the objectives of the NODEs which would not be done by private entities. Regulation would be another function which would require resources. A regulatory body, set up under a law should have its established channels of funds along with increasing the accountability of such a body. The channels of funds can include, a) Government finances, b) Transaction fee levied on private entities for using the NODEs framework. The Economic Survey 2018-2019 proposed monetising of select government data.[23] Monetising of government data is also being considered under the Smart Cities Mission.[24] The financing model should take into consideration accessibility of services to population at large while not excluding smaller service providers. It would be essential to ensure that access to public goods is not obstructed by such fee structures.

   There are strengths and weaknesses in various models and an ultimate decision should be taken after considering the ability of a model to ensure transparent and accountable governance and maintain financial independence.

9. *Participatory co-design and co-creation:* In accordance with our general comments above, we believe that the principles of participatory co-design and co-creation could be extended to the "platform infrastructure" layer and should not be restricted merely to higher levels of the stack.

10. *Analytics driven, learn continuously:* Appropriate policies will need to be implemented to ensure appropriate sharing and prevent misuse of analytics data. Ensuring appropriate governance regimes pertaining to explainability of AI solutions (to prevent discriminatory and other negative outcomes),

[23] See, Ministry of Finance, 2020.

[24] See, Nath, 2019.

and appropriately apportioning liability will be essential in creating an equitable and vibrant ecosystem. As misuse of analytics data have strong societal repercussions, this should be achieved through a legal framework which would be applicable across NODEs. This would fix liability

11. *Grievance redressal:* Grievance redress mechanisms must be citizen centric - with ease of use / accessibility, responsiveness, appropriate allocation of responsibilities through implementing clear liability and responsibility frameworks, etc. being some key metrics to consider. Grievance redress processes must be accessible through physical as well as digital means. The role, jurisdictions and expertise of existing regulatory institutions will need to be appropriately considered and adequate avenues for interaction between existing and proposed regulators (and grievance redress mechanisms) must be provided. An appropriate regulatory body formed under a law would help in increasing accountability towards the citizen. The legal framework setting up the regulatory body should delineate liability and responsibilities in performing grievance redressal.

4 Response on delivery platforms

Question 3: What are the biggest challenges that may be faced in migrating from a GovTech 1.0 or 2.0 approach to a NODE approach? How might these be overcome?

The CW adopts a somewhat 'solutionist' approach to percieved problems in multiple sectors without an adequate exploration of the problems faced in each sector / the interaction of existing institutional frameworks in each sector, etc. It will therefore be important for any proposed NODE to first determine and clearly delineate the purpose and scope of a NODE and the aims sought to be achieved thereby. This would enable better protection of fundamental rights, better regulatory and technical design, and prevent mission creep. It would also enable a more holistic or comprehensive consideration of suitable/alternative options and also provide a roadmap against which to measure success of any intervention.

Challenges that could be faced in migration of platforms could include:

- Institutional inertia, including due to the high degree of coordination likely to be required between different ministries/departments of the government, including at state and local levels. There will also be a need to ensure appropriate regulatory coordination between different agencies/regulators.

- Lack of state capacity to adequately identify and tag relevant data sets, clean/verify data or ensure appropriate data quality.
- Lack of standardised formats for data recording and database creation/maintenance, therefore affecting data quality and interoperability of systems.
- Possible negative impacts on fundamental rights (exclusions, discrimination, privacy, etc.).
- Lack of competition in a sector owing to onerous licensing conditions for the private sector.
- Lack of digital literacy of the targeted participants of the concerned node.
- Problems with migration from existing systems and standards, maintenance of databases and web-services etc.
- Problems with citizens being able to access grievance redress mechanisms (due to frictions, information asymmetry, etc.) etc.
- Lack of trust in digital systems mandated by the government.
- It will also be important to ensure that any smaller digitisation/e-governance projects are not ignored or improved, if they do not fall under the NODEs framework.

Education and awareness, participatory and transparent design and regulatory processes, creating appropriate institutions to drive adoption of and take responsibility for platforms will be essential to ameliorate some of the problems listed above. It will be particularly important to examine weaknesses in existing digital governance/open data initiatives by the government, and learn from experience.

It will also be essential to carry out a detailed analysis of the legal[25] and policy[26] frameworks that already exist in any given sector so as to be able to (a) ensure consistency with existing constitutional and statutory frameworks, (b) learn from and seek to avoid problems with existing e-governance platforms in any particular sector.

Question 4: In your opinion, should all delivery platforms be open source or are Open APIs and open standards sufficient? Please elaborate with examples.

[25] Such as under the Right to Information Act, 2005, the Information Technology Act, 2000, the proposed Personal Data Protection Bill, etc.

[26] Such as those pertaining to Digital India, the National Digital Communications Policy, policies pertaining to the use and adoption of open source software, open APIs, etc

As mentioned in our comments on guiding principles number one (1) above, the state must focus on opening up data through the use of open source solutions. Consistency with existing policies pertaining to use of OSS, Open APIs, etc. must be maintained in the development of any state-led solutions/platforms - both to build databases/ensure appropriate record keeping and data maintenance, as well as to permit access to data sets. As an example, the United Kingdom National Digital Twin (NDT) initiative which seeks to build digital representation of assets, processes or systems along very similar lines of India's NODEs architecture also embraces openness as a key design principle. According to the Gemini Principles that are supposed to form the backbone of this initiative, *"The NDT must be based on open standards, industry best practices and open application programming interfaces (API) to allow a vendor-neutral approach, with industry-agreed architecture models."*[27]

Further, we note that the practice of opening up government data and providing access with the help of open APIs is already being adopted by many countries. For instance, the European Union has an open data portal which provides access to data from EU bodies for both commercial and non-commercial purposes.[28] Similarly a number of latin american nations have open data portals which use open source APIs.[29]

5 Response on governance

Question 5: 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, eg: financing, procurement, data sharing.

While certain high-level common principles (such as the need to protect fundamental rights by ensuring that all regulations satisfy the constitutional tests, need to ensure accountable institutional frameworks, the manner in which granular and informed consent will be obtained for processing and sharing of data, appropriate mechanisms to ensure consultative and transparent regulation making processes etc.) may be put in place for all NODEs to adhere to, each sector will require its own governance framework based on the scope and aims of the platform/NODE,

[27] Digital Built Britain, 2018.

[28] *EU Open Data Portal*, 2012.

[29] Steinberg and Castro, 2017.

the possible market failures that may arise in the sector, the political economy of the sector, the types of data being collected and processed in a sector, the relevant authorities/institutions already existing in the sector, etc.

Particularly with regard to AI and discrimination, it is suggested that while each NODE should be cognisant about addressing issues of individual and group discrimination resulting from the processing of personal and non-personal data, the understanding of what amounts to discrimination has be evolved by each NODE distinctly and will be depend on the nature of the sector and its participants.

In addition, we recommend that before creating and the implementing a NODE, a detailed analysis be carried, so as to clearly define the aims and purposes of the NODE, as well as to understand the possible gains and problems. Any such analysis should therefore involve:

- *An open and transparent consultation process:* The conceptualisation and implementation of every NODE should also be preceded by an open and transparent consultative process which provides an opportunity to stakeholders in the sector and civil society to give their inputs on the need for and design of the sectoral NODE. This consultation process should be preceded by a consultation paper that outlines the objectives of the NODE, the problems it seeks to solve, and the technical and legal architecture of the NODE. Relevant policy proposals must be released in draft form for open comment, before being finalised. The stakeholders should be allowed a reasonable time period to submit their comments and counter comments on the the consultation paper/draft policies/draft regulations.
- *Cost-benefit analysis:* Before conceptualising a NODE and designing its architecture, it is critical for the relevant policy framers to engage in a formal and transparent cost-benefit analysis of the sectoral NODE. Therefore, a cost-benefit analysis should be appended to the the consultation paper for each node. This cost-benefit analysis should identify the market failure addressed by the NODE, assess the cost of interventions proposed by the NODE to rectify these failures and compare them with the benefits of the proposed intervention.[30]

Question 6: Are you aware of any innovative financing models that could be deployed to build NODEs? If yes, please describe along with examples eg: PPP models or community crowdfunded models

Please refer to our comments on guiding principle eight (8), above.

[30] Ministry of Finance, 2013.

Question 7: What are some potential risks that open digital ecosystems can leave citizens vulnerable to, for example, risks related to data privacy, exclusions, having agency over the use of their data etc? What types of overarching guidelines and / or regulatory frameworks are required to help mitigate them?

The creation of NODEs platforms are likely to significantly impact fundamental rights - not least those under Articles 14, 19 and 21 of the Constitution.

For instance, each of the NODEs will invariably result in the collection and processing of personal data and non personal data by both government and private entities. The collection and use of personal data by different entities must necessarily satisfy the tests laid down by the Supreme Court in the Puttaswamy decisions (2017 and 2018).[31] Equally, the impact of implementation of NODEs on the rights derived from the right to equality guaranteed under Article 14 and right to life and personal liberty guaranteed under Article 21, particularly concerns regarding equitable access to resources/services, possible exclusions of certain marginalised groups therefrom, and concerns stemming from the discriminatory impact of algorithmic decision making must be considered in the design and governance mechanisms pertaining to NODEs.

The Supreme Court has held that all fundamental rights are enacted for the larger public interest, and no individual *"can barter away the freedoms conferred upon him by the Constitution"*.[32] Therefore, the impact of collection, processing of personal data or otherwise mandating use of digitised solutions on the fundamental rights of citizens has to adequately be considered, independent of the issues of consent.

While it goes without sayind that the NODEs framework will need to be aligned with and build on the Personal Data Protection legislation that is currently pending before the Parliament, issues pertaining to data ownership and control will also need to be clarified by the governance framework of NODEs.

This is important particularly where it comes to data sets involving personal data of citizens (which are gathered by government entities using coercive powers) or data belonging to certain communities or even private entities. It is also critical for the governance framework to clarify the ownership and IP rights in products arising from processing of personal and non-personal data collected within the NODEs framework.[33] A regulatory framework would therefore be required for opening up

[31] That is, any interventions in this regard must be backed by law, be necessary to meet a legitimate State aim, be proportionate in nature, and contain relevant procedural fetters to prevent against abuse(Puttaswamy v. Union of India, 2017).

[32] *Olga Tellis v. Bombay Municipal Corporation*, 1986.

[33] Collection and processing of non-personal can impact property rights of private parties,

and permitting the processing of non-personal data. The Government has already begun the work of setting out this regulatory framework by the constitution of the Committee on Data Governance Framework.[34] Therefore we recommend that the NODEs architecture is aligned with / builds on the regulatory framework proposed by this committee.

Apart from the impact on fundamental rights of citizens, any NODE project must also consider its impact on existing constitutional design such as that of the division of subject matter competencies between state and central governments. One could envisage benefits arising from NODEs in areas such as agriculture, judicial services, education, healthcare etc. However, it must be kept in mind that sectors such as public health, land, judicial services (except the Supreme Court) amongst others, fall under the State List in the Seventh Schedule to the Constitution. The need to ensure coordination and cooperation between agencies at different levels of government in order to implement NODEs in various sectors should not result in de facto centralisation of federated competencies, including to the detriment of local self-governance processes.

In light of the above, we recommend that in order to mitigate the potential risks of open digital ecosystems, each NODE ought to be backed by an appropriate statute, to the extent possible. Not only will this ensure greater democratic deliberations, but prevent excessive and arbitrary executive action, set out the rights of citizens and private entities, and clarify the scope/limits of any particular project, (i.e. this would help prevent mission creep, while clearly delineating rights and duties, governance processes, grievance redressal mechanisms, etc).[35]

6 Response on community

Question 9: Are you aware of any end-user adoption and engagement models that platforms have successfully adopted eg feedback loops, crowdsourcing use cases, offline awareness and onboarding campaigns?

competition in the digital market, and also impact individual privacy, particularly in situations where unrelated data sets are processed to reveal personally identifiable data points (Bailey et al., 2020b). Research also highlights that there is possibility of anonymised data sets being re-identified through advanced computing, or on being merged with or added to new information to reveal personal data.

[34] Ministry of Electronics & Information Technology, 2019.

[35] For instance, the statutory mandate provided to the Unique Identification Authority of India and the provisions pertaining to data sharing in the Aadhaar Act have proven invaluable in ensuring that biometric and other data is not made freely available for non-Aadhaar purposes by the public sector, including for instance, in criminal investigations.

We note that the Government already has in place a Framework for Citizen Engagement in e-Governance, which can be updated/revised and strengthened going forward.[36]

Given the adoption of e-Governance systems globally over the past two decades, there is significant literature on user-adoption and participation models applied the world over. Of importance however, will be the need to recognise motivations for citizen participation, building end-user trust in systems,[37] ensuring that projects are actually built in a citizen-centric manner (including by public institutions genuinely sharing agenda setting and decision making power), developing inclusive processes through inception, development and roll-out processes, developing services for the most marginalised, etc.[38]

7 Response on support required

Questions 12, 13, 14:

The CW provides a basic overview of the concept of a 'NODE' and identifies certain sectors in which such a system could lead to (efficiency) gains. However, greater clarity is required on the need for such interventions on the scale envisaged in the document, particularly in view of the centralised, stack based approach proposed in the CW. We would prefer if specific cases/sectors were provided, and the scope/aims of specific NODEs could be examined in greater detail. This could also lead to the crystallisation of general principles that may be applicable across NODEs.

Given the complexity and scope of the proposed NODEs related intervention, the present document should be seen as an initial/exploratory document that seeks to provide conceptual clarity on the scope and purposes of the NODEs ecosystem as a whole. The resulting recommendations must, rather than prescribing substantive recommendations (pertaining to individual NODEs), focus on procedural

[36] Notably, the Framework recognises the need for a well thought out process for citizen engagement that considers the needs of citizens, the relevant degree of engagement sought, etc. The Framework also points to the need for more transparent/participatory decision making, creation of a citizen engagement fund, and development of an engagement toolkit. The success in implementation of the Framework is however uncertain.

[37] Through improving usability and service provision, providing greater and better quality information, providing easy grievance redress, ensuring security of data, limiting exclusions, ensuring proper and robust functionality, etc.

[38] See generally, (LeBlanc, 2020) and (Zambrano, Lohanto, and Cedac, 2009).

issues concerned with how different stakeholderscan be included in the design and conceptualisation process for each NODE.[39]

As far as future engagement is concerned, we would appreciate the opportunity for greater interaction with sectoral/technical experts and other stakeholder groups on perceived problems and solutions, as well as interaction with policy makers / regulators, particularly to understand the institutonal and other reasons for slow or improper delivery of existing e-Governance initiatives.

We are eager to continue to participate in this process and would be happy to engage in both knowledge building sessions as well as through consultation processes (whether virtual or physical).

[39] Ensuring appropriate citizen engagement will not only improve regulatory design and allow a more balanced consideration of interests, but would engender greater trust and buy-in from the public at large.

References

Bailey, Rishab and Trishee Goyal (2019). *Fiduciary Relationships as a means to protect privacy: Examining the use of the concept in the draft Personal Data Protection Bill, 2018*. URL: http://datagovernance.org/files/research/NIPFP_Rishab_Trishee_fiduciaries_-_Paper_4.pdf.

– (2020). *Fiduciary Relationships as a means to protect privacy: Examining the use of the concept in the draft Personal Data Protection Bill, 2018*. URL: https://blog.theleapjournal.org/2020/01/fiduciary-relationships-as-means-to.html.

Bailey, Rishab et al. (2020a). *Comments on the draft Personal Data Protection Bill, 2019: Part I*. URL: https://blog.theleapjournal.org/2020/04/comments-on-draft-personal-data.html.

– (2020b). *Comments on the draft Personal Data Protection Bill, 2019: Part II*. URL: https://blog.theleapjournal.org/2020/04/comments-on-draft-personal-data_10.html.

Barlow, Mike and Cornelia Levy-Bencheton (2018). *The smart nation where everyone owns their personal data*. URL: https://www.smartcitiesworld.net/special-reports/special-reports/the-smart-nation-where-everyone-owns-their-personal-data.

Chunduri, Aditya (2020). *VAHAN data used to 'target' Muslims*. URL: https://www.deccanchronicle.com/nation/current-affairs/290220/vahan-data-used-to-target-muslims.html.

Digital Built Britain, Centre for (2018). *The Gemini Principles*. URL: https://www.cdbb.cam.ac.uk/system/files/documents/TheGeminiPrinciples.pdf/.

EU Open Data Portal (2012). URL: https://data.europa.eu/euodp/en/home (visited on May 27, 2020).

FICCI and KPMG (2014). *Skilling India: a look back at the progress, challenges, and the way*. URL: http://ficci.in/spdocument/20405/FICCI-KPMG-Global-Skills-report.pdf.

Health Information Technology for Economic and Clinical Health Act (2009). URL: https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/hitechact.pdf (visited on May 26, 2020).

LeBlanc, David (2020). *E-participation: A Quick Overview of Recent Qualitative Trends*. URL: https://www.un.org/esa/desa/papers/2020/wp163_2020.pdf.

Malavika Raghavan and Anubhutie Singh (2020). *Building safe consumer data infrastructure in India- Account aggregators in the financial sector- Part I*. URL: https://www.dvara.com/blog/2020/01/06/building-safe-consumer-data-infrastructure-in-india-account-aggregators-in-the-financial-sector-part-1/.

Michaelson, Rosa (2017). “Is Agile the Answer? The Case of UK Universal Credit”. In: *Grand Successes and Failures in IT. Public and Private Sector. IFIP Advances in Information and Communication Technology.* (Bangalore). Ed. by Y K Dwivedi et al. Springer. ISBN: 1-59593-322-0. URL: https://hal.inria.fr/hal-01467785/document (visited on May 27, 2020).

Ministry of Electronics & Information Technology (2019). *Constitution of a Committee of Experts to deliberate data governance framework.* URL: https://meity.gov.in/writereaddata/files/constitution_of_committee_of_experts_to_deliberate_on_data_governance_framework.pdf.

Ministry of Finance (2020). *Economic Survey 2018-19.* URL: https://www.indiabudget.gov.in/budget2019-20/economicsurvey/doc/vol1chapter/echap04_vol1.pdf (visited on May 27, 2020).

– (2013). *Handbook on adoption of governance enhancing and non-legislative elements of the draft Indian Financial Code.* Report. Ministry of Finance. URL: https://dea.gov.in/sites/default/files/Handbook_GovEnhanc_fslrc_2.pdf.

Ministry of Health and Family Welfare (2016). *Notification of Electronic Health Records (2016) for India.* URL: https://main.mohfw.gov.in/sites/default/files/EMR-EHR_Standards_for_India_as_notified_by_MOHFW_2016_0.pdf (visited on May 27, 2020).

– (2019). *National Digital Health Blueprint.* URL: https://www.nhp.gov.in/NHPfiles/National_Digital_Health_Blueprint_Report_comments_invited.pdf (visited on May 26, 2020).

Ministry of Rural Development (2013). *Ajeevika Skills Guidelines.* URL: http://ddugky.gov.in/sites/default/files/SOP/2Aajeevika_Skills_Guidelines_English_2013.pdf.

Nath, Damini (2019). “Ministry plans to go from open platform to eventual monetisation of cities' data”. In: URL: https://www.thehindu.com/news/national/ministry-plans-to-go-from-open-platform-to-eventual-monetisation-of-cities-data/article29385873.ece (visited on May 27, 2020).

Olga Tellis v. Bombay Municipal Corporation (1986). URL: https://indiankanoon.org/doc/709776/ (visited on May 27, 2020).

Personally Controlled Electronic Health Records Act (2012). URL: https://www.legislation.gov.au/Details/C2012A00063 (visited on May 26, 2020).

Puttaswamy v. Union of India (2017). 2017 (10) SCC 1.

Steinberg, Michael and Daniel Castro (2017). *The State of Open Data Portals in Latin America.* URL: https://www.datainnovation.org/2017/07/the-state-of-open-data-portals-in-latin-america/.

The Open Source Initiative (2017). *The Open Source Definition.* URL: https://opensource.org/osd.

West Bengal, Government of (2019). *Department of Technical Education, Training and Skill Development.* URL: http://www.wbtetsd.gov.in/about.

Zambrano, Raul, Ken Lohanto, and Pauline Cedac (2009). *E-governance and Citizen Participation in West Africa: Challenges and Opportunities.* URL: https://tinyurl.com/yd3spo7s.