॥न्यायस्तत्र प्रमाणं स्यात्॥

NATIONAL LAW UNIVERSITY DELHI

Prof. (Dr.) Ranbir Singh
Vice-Chancellor

May 29, 2020

Shri Ajay Prakash Sawhney
Secretary
Ministry of Electronics and Information Technology
Government of India
Electronics Niketan,
6, CGO Complex,
Lodhi Road, New Delhi – 110003

Subject: Submission of Comments for the Whitepaper on Strategy for National Open Digital Ecosystems (NODE)

Dear Mr. Sawhney,

The National Law University Delhi instituted by Act No. 1 of 2008 of National Capital Territory of Delhi is a public funded university established by the Government of NCT of Delhi on the initiative of the High Court of Delhi. The University established the Centre for Communication Governance (CCG) in 2013 to ensure that Indian legal education establishments engage more meaningfully with information law and policy, and contribute to improved governance and policymaking. CCG is the only academic research Centre dedicated to working on the information law and policy in India and in a short period has become a leading centre on information policy in the region.

The *Technology and National Security* team at the Centre looks at the role of international and domestic law in India's national security matters from a legal and policy perspective with a particular focus on cybersecurity and cyber conflict. It aims to build a better understanding of national security issues in a manner that identifies legal and policy solutions that balance the legitimate security interests and national security choices with the constitutional liberties and the rule of law. Through *its Technology and Society* team, CCG seeks to embed human rights and good governance within information policy and examine the evolution of existing rights frameworks to accommodate new media and

emerging technology. It seeks to protect and expand freedom of speech, right to assembly and association, the right to dignity, and the right to privacy in the digital age, through rigorous academic research, policy intervention, capacity building, and supporting strategic litigation.

We regularly engage with government ministries and commissions such as the Ministries of External Affairs, Law & Justice, Information Technology, and Communications, and the Competition Commission of India, and work actively to provide the executive and judiciary with useful research in the course of their decision-making on issues relating to information policy.

As part of our work, and given how critical it is to provide policymakers with well researched and useful material, we are submitting our response to the Whitepaper on Strategy for National Open Digital Ecosystems (NODE). We welcome the opportunity to comment on the consultation whitepaper and commend MeitY for adopting a public and consultative approach to the whole process.

We hope that the response is of assistance to MeitY. My colleague Ms. Smitha Krishna Prasad (smitha.prasad@nludelhi.ac.in) and Shashank Mohan (shashank.mohan@nludelhi.ac.in) can provide any additional material required, and we are happy to offer any further support to MeitY.

With warm regards,
Yours sincerely,

Ranbir Singh

(A University of Law Established in 2008 by Act No. 1 of 2008 of Delhi)
Sector-14, Dwarka, New Delhi - 110 078 ☎ :+91 11 2803 4253 🖷:+91 11 2803 4256
✉: ranbirsingh2107@gmail.com, vc@nludelhi.ac.in website: http://nludelhi.ac.in

CENTRE FOR COMMUNICATION GOVERNANCE AT NATIONAL LAW UNIVERSITY DELHI

COMMENTS TO MEITY ON THE CONSULTATION WHITE PAPER ON STRATEGY FOR NATIONAL OPEN DIGITAL ECOSYSTEMS (NODE)[°]

The Centre for Communication Governance at National Law University Delhi (CCG) is an academic research centre dedicated to working on information law and policy in India through rigorous academic research and capacity building. We seek to embed human rights and good governance within communication policy to protect digital rights and advance information security in India.

We are grateful to the Ministry of Electronics and Information Technology ("MeitY") for inviting public comments and suggestions on the Strategy for National Open Data Ecosystems ("NODE") Consultation Whitepaper in March 2020 ("NODE Whitepaper / Whitepaper"). Through this submission, we hope to meaningfully contribute to MeitY's existing law and policy making efforts in an open and transparent manner.

EXECUTIVE SUMMARY

The NODE Whitepaper proposes a complex network of digital platforms with the aim of providing efficient public services to the citizens of India. This is an ambitious project given the low levels of digital literacy and socio-economic conditions prevalent in India.

[°] Authored by ***Shashank Mohan*** along with ***Gunjan Chawla*** and ***Nidhi Singh***. The research assistance was provided by ***Vagisha Srivastava***, ***Palash Srivastava***, ***Nitya Bansal*** and ***Ritika Bansal***, and the document was reviewed by ***Smitha Krishna Prasad***.

The NODE runs into several challenges arising from data privacy and security, as well as the lack of clarity on openness, transparency and accountability around public-private relations, independent regulatory and governance structure, and the potential for exclusion of citizens from public service benefits.

Although the NODE architecture is fraught with such challenges, we have prioritised subject areas which are most relevant to our prior work and expertise while drafting these comments. We have analysed and provided recommendations from a law and policy perspective, keeping constitutional principles, cyber security concerns, and global best practices at the forefront.

We believe that the NODE Whitepaper stops short of providing a robust definition of openness, and does not comprehensively address existing Government policies on open source software and open APIs. We recommend that existing policies are adopted where relevant, and are revised and updated at least in the context of NODEs where required.

One of the key concerns with the NODE Whitepaper is the lack of detailed discussion on the aspects of data privacy and security. The Whitepaper does not consider the principles of data protection established in the Personal Data Protection Bill, 2019 ("PDPB 2019"), or take into account other internationally recognised principles. Without adequately addressing the data privacy concerns which arise from NODEs, any policy framework on the subject runs the risk of being devoid of context. The existence of a robust privacy framework is essential before instituting a NODE like architecture. As the PDPB 2019 is considered by Parliament, MeitY should as a minimum incorporate the data protection principles as laid down in the PDPB 2019 in any policy framework for NODEs. In order to fully protect the right to privacy, and autonomy, participation in or the use of NODEs must be strictly voluntary.

A NODE framework built with the aim of public service delivery should also incorporate principles of transparency and accountability at each level of the ecosystem. In a network involving numerous stakeholders including private entities, it is essential that the NODE architecture operates on sound principles of transparency and accountability

and sets up independent institutions for regulatory and grievance redressal purposes. Public private relationships within the ecosystem must remain transparent in line with the Supreme Court jurisprudence on the subject. We recommend that each NODE platform should be supported and governed by accountable institutions both at the central level, in a transparent manner. These institutions must be independent and not disproportionately controlled by the Executive arm of the Government.

Lastly, we focus on the importance of inclusion in a digital first solution like the NODE. Despite steady growth in Internet penetration in India, more than half of its population does not enjoy access to the Internet and there is a crucial gender gap in the access to Internet amongst Indians, with men forming a majority of the user base. Learning from studies on the challenges of exclusion in relation to the Aadhaar project, we recommend that the NODE architecture must be built keeping in mind the realities of India's digital infrastructure. Global best practices suggest that designing frameworks which are based on inclusion is a pre-condition for building successful models of e-governance. Similarly, NODEs should be built with the aim of inclusion, and must not become a roadblock for accessing public services by citizens.

We would like to thank MeitY for providing us with an opportunity to comment on the NODE Whitepaper and would like to express our interest in participating in any future consultation/ discussion the Ministry conducts on this subject.

TABLE OF CONTENTS

INTRODUCTION

We have drafted our comments to the NODE Whitepaper focusing on the issues of data privacy, governance and security. Highlighting the law and policy challenges around establishing a complex NODE ecosystem in India, we have provided our recommendations on indicators that MeitY should take into consideration before finalizing the NODE architecture.

We appreciate the detailed questions listed by MeitY in the NODE Whitepaper, but have approached our comments in thematic manner which best capture our expertise and subject area of work. We have divided our key concerns into four broad categories:

1. Open standards for building NODE
2. Privacy and security
3. Transparency and accountability
4. Community Engagement

Each section contains a detailed analysis from the perspective of law and policy and a set of recommendations which must be considered by MeitY while developing the NODE architecture.

We have relied on both primary sources of information, such as legislation, case law, and policy documents and secondary sources such as scholarly articles and media reportage.

1. Open standards for building a NODE ecosystem

We acknowledge and welcome the emphasis on open standards in any policy proposal for building a comprehensive e-governance model for public service delivery in India. While open standards in e-governance models will increase transparency and offer opportunities for collaboration between various stakeholders, it is essential to clearly lay down the principles of open standards in a policy document like the NODE Whitepaper.

As of now, it is not clear what the NODE Whitepaper means by various terms like, open standards, interoperability, or modular architecture. The term 'open' is defined as referring to principles of openness, including transparency, accessibility, interoperability, open APIs, standards, and open source code (where appropriate). However, the Whitepaper envisions different degrees of openness for each NODE.

A. Open source, APIs, and standards

The Whitepaper defines 'NODE' as 'open and secure delivery platforms, anchored by transparent governance mechanisms, which enable a community of partners to unlock innovative solutions, to transform societal outcomes'. The Whitepaper envisions NODEs to be shared, open, and modular platforms, based on open APIs, open standards, open data and modular architecture. Although the Whitepaper defines the word 'open', it does not explain what is meant by principles of openness, open standards, open APIs, and open source code. Some terms and related principles of open source software and open APIs, and have been laid out by existing Government policies, but the NODE Whitepaper does not discuss or establish a connection with these policies.

The Policy on Adoption of Open Source Software for Government of India (2014)[1] ("OSS Policy") refers to the more widely understood concept of Free and Open Source Software (FOSS), in its definition of 'open source software'. Under the OSS policy, 'open source' refers 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

[1] Ministry of Communication & Information Technology, Policy on Adoption of Open Source Software for Government of India (Department of Electronics & Information Technology, F. No. 1(3)/2014 – EG II) <https://meity.gov.in/writereaddata/files/policy_on_adoption_of_oss.pdf> accessed on 28 May 2020.

modified software (without having to pay royalties to previous developers). One of the core objectives of the OSS Policy is 'to ensure strategic control in e-Governance applications and systems from a long-term perspective'. We recommend that any policy framework for NODEs should not only require the use of open source software, but also clearly define and illustrate the standards for open source code, and its incorporation in NODEs.

Similarly, the Policy on Open Application Programming Interfaces (APIs) for Government of India[2] ("Open API Policy"), states that all Government organisations shall adopt 'Open APIs' to enable quick and transparent integration with other e-Governance applications and systems implemented by various Government organizations. Similar to the concept of open source codes discussed above, policy frameworks for NODEs must clearly define and establish the contours of open APIs, and standards for adoption of such open APIs in NODEs.

The India Enterprise Architecture Framework[3] ("IndEA Framework") of MeitY, which targeted the establishment of a new e-governance model in India, clearly adopted existing Government policies on open source (OSS Policy) and open APIs (open API Policy) as the basis for the application architecture of its model[4]. The NODE Whitepaper does not demonstrate how it intersects with the IndEA Framework and whether it is an extension or replacement to the model suggested therein.

MeitY should clearly define what the principle of 'openness' in the context of NODE, describing in detail its scope and application to specific aspects of the ecosystem, such as source codes, APIs, and other standards. Existing policies such as the OSS Policy and the Open API Policy offer guidance on these subjects. However, many of these policies are dated, and could require review – for instance the OSS Policy and the Open

[2] Ministry of Communication & Information Technology, Policy on Open Application Programming Interfaces (APIs) for Government of India (Open API policy) (Department of Electronics & Information Technology, F.No. 1(4)/2014-EG II) <https://meity.gov.in/writereaddata/files/Open_APIs_19May2015.pdf> accessed on 28 May 2020.
[3] Ministry of Electronics and Information Technology, 'The India Enterprise Architecture Framework (IndEA) 2018', <https://meity.gov.in/india-enterpise-architecture-indea> accessed on 28 May 2020.
[4] Ibid, ch 6 para 6.6.1

API Policy are both over 5 years old. We recommend that MeitY, should take this opportunity to update these policies, or establish fresh standards for such principles within the policy framework for NODEs, at the very least. Clarity on the principles of openness will bring transparency and help build trust among citizens and businesses, both of which are key stakeholders in developing the NODE ecosystem.

B. International best practices

The e-Governance projects of countries such as Estonia[5], the United Kingdom[6], and Austria[7] have adopted the use of open source software for greater transparency and cross collaboration. India should learn from the experiences of these nations while framing its novel e-Governance strategy. The United Nations, in its E-Government Survey, 2018 ("UN e-Gov Survey/ the Survey")[8] also acknowledges the importance and benefits of adopting open source software technology in e-gov projects. The survey document notes that open source service platforms aid efforts in collaboration for producing public value and contributing to society in furthering the common good.

CCG recommendations

- The term 'open' as it applies in the context of the NODE ecosystem must be clearly defined, describing in detail its scope and application to specific aspects of the ecosystem, such as source codes, APIs, and other standards. This will help meaningful participation by private players and citizens and assist in achieving the goal of interoperability.

[5] Enterprise Estonia 'e-Estonia guide' <https://e-estonia.com/wp-content/uploads/eestonia -vihik-a5-200303.pdf> accessed on 28 May 2020.
[6] HM Revenue & Customs, ' Open Data Strategy' (June 2012) <https://assets.publishing.service.gov.uk /government/uploads/system/uploads/attachment_data/file/89258/open-data-strat.pdf> accessed on 28 May 2020.
[7] Federal Chancellery and Federal Ministry of Science, Research and Economy, 'Digital Roadmap Austria' <https://www.digitalroadmap.gv.at/fileadmin/downloads/digital_road_map_broschuere_eng.pdf> accessed on 28 May 2020.
[8] United Nations Department of Economic and Social Affairs, 'E-Governance Survey Data 2018' (UN E-Government Survey 2018) <https://publicadministration.un.org/en/research/un-e-government-surveys> accessed on 28 May 2020.

- Established principles laid down in the OSS Policy and the Open API Policy may be adopted, or MeitY could adopt set fresh standards for such principles as may be required.

- Adhering to established open source standards would aid transparency and help in making platforms reusable, shareable and modular, as envisioned by the NODE architecture.

- Internationally recognized best practices on open standards should be referred to and adopted within the context of the NODE ecosystem. .

2. Privacy and Security

Digital delivery platforms are one of the key features of NODE as envisioned in the Whitepaper. Beyond being modular and interoperable, these platforms will rely on data sharing between various departments of the government for seamless service delivery. Such data will include the personal data of citizens and individuals obtaining public services through the NODE. The NODE Whitepaper argues that unbridled data flows between government departments will enable single touch points for data collection, thereby smoothening public service delivery. The framework envisions the participation of the private sector as well, wherein private players shall be permitted to build novel services and solutions on top of the NODE delivery platforms. It is unclear from the NODE Whitepaper, as to how data will be shared within government departments or with private players or its protection guaranteed in such a complex web. This approach raises concerns around data privacy and security. The NODE Whitepaper does consider the importance of data privacy and security and recognises the privacy risks associated with instituting a data driven NODE. However, it does not comprehensively consider data protection principles as laid down by the Personal Data Protection Bill, 2019 or other internationally recognised models and best practices.

A. Data privacy

In an elaborate e-governance ecosystem, it is reasonable to demand the seamless flow of data between government departments as a key feature of service delivery. However, such data flows should not be enabled at the risk of digital privacy and security.

The right of control and autonomy over one's personal data and information was emphatically recognized in the Supreme Court's landmark judgment in *K.S. Puttaswamy v. Union of India*[9] ("*Puttaswamy I*").[10] Informational control and the right of choice over the dissemination of personal information was acknowledged to be a distinct factor of the larger privacy right enjoyed by individuals.[11] Consent was considered to be central

[9] KS Puttaswamy and Anr. vs Union of India (2017) 10 SCC 1, para 184.
[10] Id. para 141.
[11] Id. paras 169-169.

to the protection of informational privacy along with the requirement of transparency, wherein data recipients were obligated to disclose information related to data transfer and use.[12] Sanjay Kishan Kaul, J. while discussing the right to informational privacy stated that, "*The hallmark of freedom in a democracy is having the autonomy and control over our lives which becomes impossible, if important decisions are made in secret without our awareness or participation.*"[13]

Whereas Indians do have a fundamental right to privacy (which affords their data some protection before constitutional courts), they do not enjoy the protection of a comprehensive data privacy law, despite the Supreme Court's recommendations on the subject in *Puttaswamy I*[14]. After going through two iterations, the Personal Data Protection Bill, 2019 ("PDPB 2019") is currently before a joint parliamentary committee for recommendations, before it is considered by Parliament. The PDPB 2019 has been proposed as legislation for the protection of personal data of Indians against both public and private entities.

The existence of an exhaustive data protection framework, which applies to both the public as well as private institutions is an essential component of a data dependent e-governance system, on the lines of the NODE [15].

The PDPB 2019 recognizes certain data protection principles such as purpose limitation,[16] collection limitation,[17] notice[18] and consent,[19] security,[20] and transparency[21]

[12] Id. para 184.
[13] Id. para 53 (Sanjay Kishan Kaul J.'s opinion).
[14] KS Puttaswamy and Anr. vs Union of India (2017) 10 SCC 1
[15] As per the UN E-Government Survey 2018, one of the main criteria for establishing a resilient e-government project is data protection and ensuring the privacy of individuals, communities, and specific groups from unauthorized surveillance and discriminatory monitoring, UN E-Government Survey 2018 (n 8).
[16] The Personal Data Protection Bill, 2019, cl 5 <http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf> accessed 28 May 2020.
[17] Id. cl 6
[18] Id. cl 7
[19] Id. cl 11
[20] Id. cl 24
[21] Id. ch 6

and accountability,[22] in the interest of data principals.[23] These principles form the basis of India's privacy framework and were recognized by the Supreme Court in *K.S. Puttaswamy v. Union of India*[24] ("*Puttaswamy I*"). They were previously propounded in India by the AP Shah Committee Report of 2012[25]. These principles are also commonly accepted as the basis for data privacy frameworks across the world. At the outset, we recommend that it would be ideal to implement personal data driven systems for public service deliver, including NODEs after only after a robust data protection law is put into place. In the absence of such a law, the policy framework for NODEs should incorporate recognized data privacy principles that are expected to be implemented in such a law.

In this context, we discuss some of the additional principles recognized in the PDPB 2019 below.

a) The right to correction and erasure (clause 18): provides the data principal the right to correct, update, and erase their personal data;

b) Security safeguards (clause 24): creates an obligation on data fiduciaries to use methods like de-identification and encryption, steps necessary to protect the integrity of personal data, and steps necessary to prevent misuse, unauthorised access to, modification, disclosure or destruction of personal data;

c) Data protection impact assessment (clause 27): creates an obligation on data fiduciaries to conduct a data protection impact assessment when they wish to process personal data involving new technologies or large scale profiling or use of sensitive personal data such as genetic data or biometric data, or any other processing which carries a risk of significant harm to data principals;

[22] Id. cl 10

[23] Data principals means the natural person to whom the personal data relates, The Personal Data Protection Bill, 2019 (n 16), cl 2(14).

[24] Puttaswamy (n 9), para 184.

[25] Planning Commission, Government of India, Report of the Group of Experts on Privacy (2012) ("AP Shah Committee Report"), ch 3.

d) Audit of policies and conduct of processing (clause 29): creates an obligation on data fiduciaries to have their policies and the conduct of their processing audited annually by an independent auditor; and

e) Grievance redressal (clause 32): creates an obligation on data fiduciaries to establish a procedure and effective to redress the grievances of data principals efficiently and in a speedy manner.

Some of the challenges in the PDPB 2019[26] as well as broader legal frameworks in India, which dilute protection to data principals are discussed in Sections 2(B), 2(C) and 2(D). The NODE Whitepaper does not discuss the principles adopted by the PDPB 2019 or the kinds of data privacy risks associated with the adopting a NODE framework. At the time of submitting these comments, the PDPB 2019 is currently being considered by Parliament. While we wait for the outcome of these deliberations, we recommend that in the interim, MeitY adopts the data protection principles and safeguards as existing under the PDP 2019 as a baseline. It is relevant to highlight some of the challenges arising out of the present PDPB 2019, such as diluted standard of consent for State access and excessive exemptions for law enforcement and investigation purposes (discussed below). MeitY should consider these issues and incorporate data privacy safeguards in the NODE framework aimed at safeguarding individual autonomy as discussed in *Puttaswamy I*. It is pertinent to ensure that, in order to protect both the privacy and autonomy of citizens, NODE based public delivery systems should not be mandatory and / or the only option for citizen engagement with agencies responsible for the provision of public services and benefits.

B. Notice and consent

Notice and consent have long been considered essential principles for safeguarding data privacy rights, given the crucial role consent plays in the exercise of individual autonomy and self-determination. However, there are two broad issues with the

[26] Submissions in this section have been borrowed from the CCG's comments on the Personal Data Protection Bill, 2019, as submitted to the Joint Parliamentary Committee, which is reviewing the bill before it is considered by Parliament. The comments are protected by parliamentary privilege and therefore we have not published those.

operation of these principles in the context of India's legal framework, as well as the broader digital world.

Data privacy law

The PDPB 2019 provides for the doing away of the requirement of 'notice[27] and consent'[28] for certain kinds of data processing activities such as, (a) provision of any service or benefit from the State; (b) issuance of licenses and permits; and (c) under any law made by Parliament or State Legislature. The removal of both notice and consent requirements in these circumstances negatively impact the autonomy and choice data principals enjoy over their personal data[29]. Similar standards must be applied to data processing for private and State functions, and consent should be treated as a primary ground for processing by the private sector, the State, and for the purpose of undertaking State functions / compliance with law. Exceptions to the requirement to provide notice and obtain consent, maybe allowed in limited, defined circumstances.

However, as they relate to the processing of personal data by NODEs (whether for state service, benefit, or permit), it is important that any personal data collected and processed must adhere to the principles of notice and consent given that there is potentially a mix of private sector and State led processing of such data. For this reason, it is also important that data principals/ users may be able to withdraw their consent with the same ease with which they provided it.[30]

Consent Fatigue and the Digital World

While consent has been an established data protection principle for decades now, in the digital sphere meaningful consent remains elusive.[31] Consent forms are often

[27] The Personal Data Protection Bill, 2019 (n 16), cl 7(3).
[28] Id. cl 12.
[29] Puttaswamy (n 9), paras 141, 169, and 188.
[30] The Personal Data Protection Bill, 2019 (n 16), cl 11(1)(e).
[31] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, 'A Free and Fair Digital Economy, Protecting Privacy , Empowering Indians' ("Justice Srikrishna Committee Report") , ch 3

complicated and shrouded in legalese, making it inconvenient for regular users to engage with them, understand them, and provide their consent after evaluating the attached risks.[32] The validity of consent gets further diluted when the transaction is between the State and a citizen.[33] The Justice Srikrishna Committee observed that:

> … *When a citizen is to receive a welfare benefit, the validity of any consent given is questionable*. The problem is exacerbated if the consent is given by a person in dire need of essential services or goods. The interaction between the state and the citizen in this context cannot be compared to that of a consumer entering into a contract with a service provider. *The option available to a consumer in refusing an onerous contract and choosing another service provider is not available to a person seeking a welfare benefit from the state*.[34] (emphasis added)

Matthan in his 2017 discussion paper, *Beyond Consent - A New Paradigm for Data Protection*,[35] points to the fault lines in the consent model of data protection. He states that meaningful consent is elusive in the digital age due to the manner in which data is collected, stored, and processed. Complex contracts which are dense and not accessible to regular users, coupled with the number of such contracts which require consent, diminish informed consent. He also points to the interconnectedness of data in the online world, where privacy policies are ever changing and the risks posed by machine learning algorithms which are capable of creating meaning out of innocuous fragments of data, as a threat to the consent model.

<https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf> accessed on 28 May 2020.

[32] Id.

[33] Id. ch 8

[34] Id.

[35] Rahul Matthan, 'Beyond Consent: A New Paradigm for Data Protection', Takshashila Discussion Document, 2017-03 <https://takshashila.org.in/wp-content/uploads/2017/07/TDD-Beyond-Consent- Data-Protection-RM-2017-03.pdf> accessed on 28 May 2020

In a study[36] which evaluated the privacy policies of a few popular online services, college students were surveyed on their understanding of these policies. Scholars concluded that privacy policies are primarily drafted with a view to protect the service providers from liability claims, rather than provide the user with usable information. They found that users have little leeway in amending the contracts entered into by them and usually sign up for entire contracts in order to access the services.[37] A key finding from the study is that when policies were clearly drafted or when users can be expected to find the answers in the policy, users are more likely to evaluate privacy risks correctly.[38]

Several different solutions have been proposed to tackle the problem of meaningful consent over the years.

The Justice Srikrishna Committee Report suggests a product liability approach to consent forms, wherein, lapses by the data fiduciary will make it liable for reparation.[39] Recommendations by the Srikrishna Committee to incorporate meaningful consent included model forms of consent (approved by a regulatory authority),[40] data trust scores[41] for significant data fiduciaries, and dynamic consent renewal.[42] The Committee also recommended the concept of consent dashboards, a single point of reference for data principals to regulate their consent management, for solutions to consent fatigue and operationalise informed consent.[43] Similar to the concept of the consent dashboards, the PDPB 2019 incorporates the concept of 'consent managers' which are interoperable platforms enabling data principals to gain, withdraw, review, and manage their consent.[44]

---

[36] Rishab Bailey et al, 'Disclosure in Privacy Policies: Does "notice and consent" work?' (2018), NIPFP Working Paper No. 246 <https://www.nipfp.org.in/media/medialibrary/2018/12/WP_246.pdf> accessed on 28 May 2020.
[37] Id. p 39.
[38] Id.
[39] Id. ch 3.
[40] In this instance the proposed Data Protection Authority of India.
[41] This principle has been adopted by the Personal Data Protection Bill, 2019 (n 16) ss 7, 23, and 29.
[42] Justice Srikrishna Committee Report (n 31) ch 3.
[43] Id.
[44] The Personal Data Protection Bill, 2019 (n 16), s 23.

Another model proposed by MeitY is the Electronic Consent Framework ("ECF"), which recognizes that "it is imperative that all user data sharing is fully consented to, in electronic form, by the user(s) whose data is shared". The 'user' referred to in this is defined as "any person who wishes to share data about them[selves] for availing a service.[45]" Clearly, in the context of NODE, this 'user' would also necessarily be the intended beneficiary of the 'service or benefit' that would be provided by the Government through the NODE ecosystem. However, (as mentioned above) clause 12 of the PDPB 2019 directly contradicts this specification, insofar as it neglects the autonomy of the user by not requiring their consent for the processing of personal data.

It is of utmost importance that the consent parameters encoded into consent flows that enable data flows (as envisaged by the ECF) be clearly communicated to the user of the NODE or other e-Governance service in a human-readable manner (as opposed to machine readable) to create a trusted system for the delivery of e-Governance services. Similarly, the right to erasure on withdrawal of consent must also be encoded into the architecture.

Dan Wiese Schartum, in his paper '*Making Privacy by Design Operative*'[46] suggests that for efficient and effective incorporation of consent into a digital ecosystem, the legal standards must first be structured in a way which can be articulated through operators which are used in the processing of data – IF, AND, and THEN.

For example,

IF valid user authentication = yes,

AND tick off box for freely given consent = yes,

AND tick off box for read information = yes,

AND tick off box for consent = yes,

[45] Ministry of Electronics and Information Technology, 'Electronic Consent Framework: Technological Specifications v 1.1' at p. 3, para 3.2 <http://dla.gov.in/sites/default/files/pdf/MeitY-Consent- Tech-Framework%20v1.1.pdf> accessed on 28 May 2020.

[46] Dag Wiese Schartum, 'Making Privacy by Design Operative' (2016) 24 Int'l JL & Info Tech 151.

THEN valid consent is assumed and further processing will continue with consent as the legal basis of processing.

The success of this model depends highly upon the unambiguous conceptualization of legal standards which govern free and informed consent. The model must also be flexible enough to be updated in accordance with evolving legal standards. Users may have their information uploaded in a module which is accessible only to the user, consent may be required for extraction of data whenever needed.

Accountability frameworks, that ensure that privacy rights are protected even if notice is not completely accessible and consent is not meaningful have also been proposed[47].

The challenges around consent frameworks must be considered by MeitY while formulating policy frameworks for implementation of NODEs. The PDPB 2019 adopts a holistic approach by recognising other data protection principles like purpose limitation, collection limitation, accountability and transparency principles etc. but the proof of operationalising meaningful consent will lie in the implementation of the law. The concept of meaningful consent gets further diluted in State-citizen relations – the policy frameworks for NODEs must recognize this challenge and establish mechanisms where citizens can actively assess privacy risks before providing their consent. Lastly, an important metric to ensure autonomy of citizens would be to ensure that engagement with NODEs is voluntary.

C. Law enforcement, Security and Mass surveillance

A centralised database of user demographic information also raises concerns about mass surveillance. Projects such as the National Social Registry or the Socio-Economic Caste Census, which are Aadhaar seeded databases for maintaining a harmonised and integrated profile of Indians[48], have also been criticized as they create a significant risk

[47] See Smitha Krishna Prasad, 'Back to the Basics: Framing a New Data Protection Law for India' (January 30, 2018). <https://ssrn.com/abstract=3113536> accessed on 28 May 2020; and Matthan (n 35).
[48] Kumar Sambhav Shrivastava, 'Documents Show Modi Govt Building 360 Degree Database To Track Every Indian' (Huffpost India, 17 March 2020) <https://www.huffingtonpost.in/entry/ aadhaar-national-social-registry-database-modi_in_5e6f4d3cc5b6dda30fcd3462> accessed on 28 May 2020.

of mass surveillance, and illegal profiling of Indian citizens. With single access portals like the NATGRID[49] which seeks to collate data from ten government agencies and is expected to go live soon[50], a NODE without data protection safeguards, may prove to enhance existing surveillance powers of the Indian government. There are two distinct but interconnected concerns here: interconnection of databases and (illegal) sharing of information, and mass surveillance.

Interconnected Databases and Procedure for Sharing of Information

NODEs providing public services to individual citizens will collect and process large amounts of personal information. However, in line with data protection principles, such data should only be used for the purpose specified at the time of collection of such information. The interconnection of databases, for seamless provision of services poses a risk to this data protection model, and the privacy of citizens.

In Puttaswamy I, the Supreme Court laid down specific tests that must be met in order to infringe upon the privacy of individuals.[51]

In the Aadhaar Judgment (*Justice Puttaswamy (Retd.) and Anr. v Union of India and Ors.*[52]) ("*Puttaswamy II*") the Supreme Court struck down section 33(2) of the Aadhaar (Targeted Delivery Of Financial And Other Subsidies, Benefits And Services) Act, 2016[53], which authorised a Joint Secretary ranking officer to allow disclosure of information (collected under the Aadhaar scheme) to the Government in the interest of national security. The court held that disclosure of information in the interests of national

[49] Vijaita Singh, 'NATGRID wants to link social media accounts to central database' The Hindu (13 Sep 2019) <https://www.thehindu.com/news/national/natgrid-wants-to-link-social-media-accounts-to-central-database/article29402252.ece> accessed on 28 May 2020.

[50] 'National Intelligence Grid to be ready by early 2020' The Tribune (22 Sep 2019) <https://www.tribuneindia.com/news/archive/nation/national-intelligence-grid-to-be-ready-by-early-2020-836533> accessed on 28 May 2020.

[51] Puttaswamy (n 9); See also Centre for Communication Governance, 'Comments on the draft personal data protection bill, 2018' <https://ccgdelhi.org/wp-content/uploads/2018/10/CCG-NLU-Comments-on-the-PDP-Bill-2018-along-with-Comments-to-the-Srikrishna-Whitepaper.pdf> accessed on 28 May 2020.

[52] Justice Puttaswamy (Retd.) and Anr. v Union of India and Ors. 2018 (12) SCALE 1.

[53] Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits And Services) Act, 2016 <https://uidai.gov.in/images/targeted_delivery_of_financial_and_other_subsidies_benefits_and_services_13072016.pdf> accessed on 28 May 2020.

security must be authorised by an officer with a higher rank than of a Joint Secretary and with the consultation of a judicial officer (preferably a sitting High Court judge). The court emphasized the importance of application of judicial mind in matters of disclosure of information for national security.

Mass Surveillance

The Telegraph Act, 1885 and the Information Technology Act, 2000 govern targeted surveillance efforts for specific purposes related to law enforcement and security of the State. The much-criticized clause 35 of the PDPB 2019 proposes to permit the Central Government to exempt any of its agencies from the purview of the bill, for inter alia, the security of the State or prevention of incitement/ commission of an offence. Similarly, clause 36(a) provides that certain provisions of the Bill will not apply where personal data is processed in the interests of prevention, detection, investigation and prosecution of any offence or any other contravention of any law for the time being in force.

However, Indian law does not permit law enforcement and investigation agencies to conduct mass surveillance activities. The Justice Srikrishna Committee[54], which drafted the first iteration of India's data protection law[55], recognized this lacuna in the law and stated, "*There is no general law in India today that authorises non-consensual access to personal data or interception of personal communication for the purposes of intelligence gathering or national security. If there are any entities that are carrying out activities of such a nature without statutory authorisation (for example, solely through executive authorisation), such activities would be illegal as per the Puttaswamy judgment as they would not be operating under law.*[56]" The committee recommended that to safeguard the data privacy of Indians, the Government must consider a specific law for the purpose of intelligence gathering.

The NODE framework must take into account all such risks before enabling a mass collection of personal data and provide for checks and safeguards against the misuse of

[54] Justice Srikrishna Committee Report (n 31).
[55] Draft Personal Data Protection Bill, 2018 <https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf> accessed on 28 May 2020
[56] Justice Srikrishna Committee Report (n 31) at 124.

such data. Legal and policy frameworks that enable data processing via NODEs must clarify that personal data collected under the NODEs will not be shared with law enforcement or investigation agencies for intelligence gathering purposes unless in line with the tests laid down in *Puttaswamy I*, and be authorised by a sitting High Court judge, in line with the pronouncement in *Puttaswamy II*.

D. Aadhaar experience

Other centralised databases such as the Aadhaar system have been criticised by security researchers[57] for not being secure enough to protect the personal data of Indians from malicious actors[58]. Vulnerabilities such as sourcing Aadhaar numbers of people from masked digits published on the web and the possibility of verifying Aadhaar numbers from APIs on government websites have been reported in the public domain[59]. Security vulnerabilities on government websites[60] and proactive publishing of data related to Aadhaar (personally identifiable information and Aadhaar numbers)[61] have brought to light the type of data security challenges centralised datasets could be subjected to. These issues were exacerbated by the fact that the Aadhaar project did not have legal backing for the first six years of its existence, thereby limiting safeguards, and accountability and oversight mechanisms.

---

[57] Sunil Abraham, 'Surveillance Project' in Reetika Khera (eds), Dissent on Aadhaar: Big Data Meets Big Brother (Orient Black Swan, 2019).

[58] Rachna Khaira, 'Rs 500, 10 minutes, and you have access to billion Aadhaar details' The Tribune (4 Jan 2018) <https://www.tribuneindia.com/news/archive/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details-523361> accessed on 28 May 2020.

[59] Aria Thaker, 'Aadhaar security failure: Government web pages provide unsecured access to demographic authentication' (The Caravan, 22 June 2018) <https://caravanmagazine.in/science-technology/aadhaar-security-failure-government-webpages-provide-unsecured-access-to-demographic-authentication> accessed on 28 May 2020.

[60] Zack Whittaker, 'A new data leak hits Aadhaar, India's national ID database' (ZD Net, 23 March 2018) <https://www.zdnet.com/article/another-data-leak-hits-india-aadhaar-biometric-database/> accessed on 28 May 2020.

[61] For more information, also refer to Amber Sinha and Srinivas Kodali, 'Information Security Practices of Aadhaar (or lack thereof): A documentation of public availability of Aadhaar Numbers with sensitive personal financial information (Centre for Internet and Society, 16 May 2017) <https://cis-india.org/internet-governance/information-security-practices-of-aadhaar-or-lack-thereof/> accessed on 28 May 2020.

The Aadhaar experience poses an important learning for future projects to ensure adequate levels of security for data stored in central databases managed by the government. Audits must be conducted and transparency is paramount in how data is shared across government departments to ensure the privacy and security of this sensitive data. Policy frameworks for NODEs must provide detailed requirements for ensuring the security of data collected under the ecosystem. The NODE Whitepaper does discuss the success of Aadhaar in creating the world's largest digital identity platform, but does not delve into the learnings from its implementation which could be used for building the NODE ecosystem.

E. International Best Practices

The UN e-Gov Survey places emphasis on cybersecurity, as a key factor in the transformation to resilient e-government. It states that security measures need to protect people's data and privacy and must be incorporated from the outset, during the design phase. Some cybersecurity measures recommended by the UN e-Gov Survey are: a) adoption of laws against the misuse of ICTs for criminal and other nefarious purposes, b) integrating adequate technical capabilities in detecting and responding to cyber-attacks, and c) establishing a minimum security criteria and accreditation schemes for software applications and systems.

Reliance could be placed on the Estonian experience, which stressed on the importance of principles of privacy and security while developing its e-governance model. Despite focusing on openness, Estonia emphasized on the security of individual data and open APIs, rather than a 'free for all' open data sets approach.[62]

CCG recommendations

- An essential component of a data dependent e-governance model is the existence of a comprehensive data protection framework which sufficiently protects the privacy rights of citizens. Since the PDPB 2019 is being currently

[62] Margetts and Naumann, 'Government as a platform: What can Estonia show the world?' (Oxford Internet Institute) <https://www.politics.ox.ac.uk/materials/publications/16061/government-as-a-platform.pdf> accessed on 28 May 2020.

considered by Parliament, MeitY should incorporate the data protection principles laid down in the bill, while developing a policy framework for NODEs.

- Acknowledging the challenges arising from the current draft of the PDPB 2019, it is recommended that the data protection principles as elaborated in the PDPB 2019 are treated as a baseline, to be improved upon as required and / or permitted under the law when it does come into effect.

- While user autonomy is essential to protecting informational privacy, there are inherent challenges with processing of data based on consent. Consent forms and privacy policies are not user friendly and do not assist users in assessing levels of privacy risk their data could be subject to. Additionally, meaningful consent gets further diluted in transactions involving the State and citizens. It is essential that MeitY recognise these challenges around consent and incorporate principles and practices aimed at safeguarding citizen choice and autonomy in frameworks for NODEs.

- Best practices from around the world on data privacy and security, as well as learnings from previous experiences within India, should be adopted in order to mitigate risks of abuse.

3. Transparency and accountability

A. Transparency in public-private partnerships

The NODE Whitepaper envisions the ecosystem to be comprised of multiple stakeholders including public and private entities and the citizenry at large. Certain features of NODEs such as modular applications and stacks, will allow private sector entities to build solutions on top of open APIs, with the aim of bringing in a variety of services and added revenue.

While the participation of the private sector might bring added value to NODEs, it is equally important to ensure that public-private partnerships are not arbitrary and maintain adequate transparency, as the core objective of a NODE is to enhance public service and e-governance. Rationality, non-discrimination, and reasonableness must dictate public-private relations, as held by various judgments of the Supreme Court of India[63].

One of the earliest cases in which the Supreme Court clarified that the Government was barred from acting arbitrarily (in accordance with Article 14 of the Constitution)[64] when entering into contracts with private parties is *Ramana Dayaram Shetty v. International Airport Authority of India*[65]*(Ramana Dayaram Shetty)*. In *Ramana Dayaram Shetty* the court held that since the activities of the Government have a public element, there ought to be fairness and equality in such dealings. The court explained that whether by entering into contracts or issuing licences, there is a legal duty on the Government to act in conformity with standards which are non-arbitrary, rational, and non-discriminatory[66].

[63] Umakanth Varottil, 'Government Contracts' in Sujit Choudhary, Madhav Khosla & Pratap Bhanu Mehta (eds.), Oxford Handbook of the Indian Constitution (OUP, 2016), available at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2953560> accessed 21 May, 2020.

[64] A more recent case which upheld the scrutiny of Article 14 principles to Government contracts is Sterling Computers Limited v. M&N Publications Limited AIR 1996 SC 51.

[65] Ramana Dayaram Shetty v. International Airport Authority of India AIR 1979 SC 1628.

[66] Id. at paras 12 and 21.

In the landmark judgment of *Tata Cellular v. Union of India*[67] *(Tata Cellular)*, the Supreme Court clarified that the principles of judicial review would apply to the power of the Government to enter into contracts, in order to prevent arbitrariness and favouritism[68]. While recognising the autonomy of the Government on financial and policy decisions, the court stressed on the importance of remedying unfairness via judicial review[69]. Laying down principles for judicial review of administrative decisions made by the Government, the court in *Tata Cellular* stated that decisions made with respect to contracts must be tested by the application of the *Wednesbury Principle of Reasonableness*[70] (a doctrine from English law which asserts that decisions made by public authorities are liable to be quashed by judicial review if considered wholly unreasonable in law) and must be free of arbitrariness, bias, and mala fides[71].

In the more recent case of *Manohar Lal Sharma v. The Principal Secretary*[72], where the Supreme Court was asked to review the allocation of coal blocks, it declared that the allocation suffered from the vice of arbitrariness and legal flaws. The court arrived at the conclusion that the allocation resulted in unfair distribution of national wealth because of a lack of transparency, non-adherence of guidelines, and non-application of mind[73].

Differentiating between a contract among two private parties and a contract where one of the parties was the State, the Allahabad High Court in *Ram Dhyan Singh v. State of UP*[74] held that in instances of Government contracts, the principles of non-arbitrariness as per Article 14 of the Constitution would apply. To avoid the erosion of public confidence, the court stated that it was essential to maintain total transparency in Government contracts[75].

[67] Tata Cellular v. Union of India AIR 1996 SC 11.
[68] Id. at para 85.
[69] Id. at para 86.
[70] Id. at para 98.
[71] Id. at para 111.
[72] Manohar Lal Sharma v. The Principal Secretary (2014) 9 SCC 516.
[73] Id. at para 154.
[74] Ram Dhyan Singh v. State of UP (2004) ILR 2 All 434.
[75] Id. at para 6.

It is clear that public-private partnership cannot be arbitrary as they involve questions of appropriation of public funds. To ensure the absence of bias and mala fides, such engagements must be transparent and non-discriminatory. Since private sector involvement is a key goal for NODEs, it is essential that transparency measures such as public auctions, criteria for the selection of private contractors, the publication of names of all private parties engaged, a database of all private parties which applied/ were considered etc. are incorporated in the policy frameworks for NODEs to ensure that processes are not arbitrary in nature.

The UN e-Gov Survey states that one of key indicators of openness, transparency and accountability on the part of the Government is the provision of public mechanisms to participate in e-procurement and public bidding processes[76]. Similarly, OECD's Recommendation of the Council on Digital Government Strategies[77] ("OECD Recommendations on Digital Government"), lists down transparency, openness, and inclusiveness of government processes and operations as one of the first principles on which States should develop their digital government strategies.

B. Notional architecture of the 'National Cyberspace' and the role of NODEs

In our comments on the National Cyber Security Strategy 2020[78], we had recommended that the National Security Council Secretariat should consider demarcating the contours of 'the sovereign cyberspace', as a narrower subset of the broader realm of the 'national cyberspace', which remains and is most likely to remain a layer permeable to foreign/ external actors in the networked economy[79]. A hybrid layer of a 'sovereign protected cyberspace' naturally emerges between these two layers. The three tiers of the

[76] UN E-Government Survey 2018 (n 8) at Chapter 5 - Global Trends in e-Government.

[77] OECD, 'Recommendation of the Council on Digital Government Strategies' (Public Governance and Territorial Development Directorate, 2014), <https://www.oecd.org/gov/digital-government/Recommendation-digital-government-strategies.pdf>, accessed on 28 May 2020.

[78] The Centre's comments to the National Cyber Security Strategy 2020 can be accessed at <https://drive.google.com/file/d/14XfyXu-5sAPgzAmEaKE78vphTTfH_Y5s/view> accessed on 28 May 2020.

[79] Centre for Communication Governance at National Law University Delhi, Comments to the National Security Council Secretariat on the National Cybersecurity Strategy 2020, (January 2020) <https://ccgnludelhi.wordpress.com/2020/01/30/ccgs-comments-to-the- national-security-council-secretariat-on-the-national-cyber-security-strategy-2020/> at pp. 33-35, accessed on 28 May 2020.

'sovereign cyberspace', 'sovereign protected cyberspace' and the 'national cyberspace' can be visualised as three concentric circles, but it is important to caution that technical interconnections as well as overlaps dependencies across the three layers remain operational, even essential (see Figure 1 below).

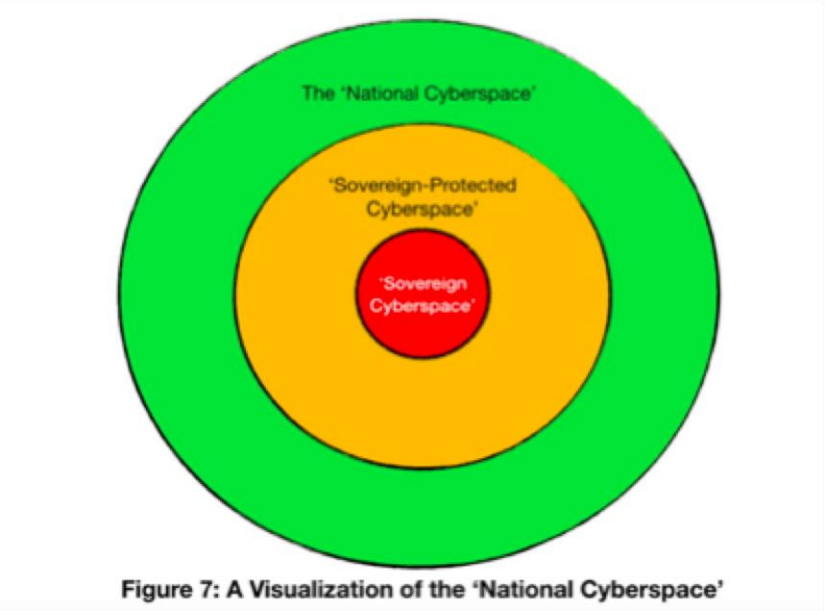

Figure 7: A Visualization of the 'National Cyberspace'

(Figure 1)

The narrow realm of the 'sovereign cyberspace' is characterised by a high degree of State control over ICT equipment and its use, is most suitable for use by the defence and security establishment of the State[80].

Notionally, the sovereign cyberspace is surrounded and supported by a larger perimeter of a 'sovereign-protected cyberspace'. Critical Information Infrastructure ("CII") is the main component of this hybrid domain, which is distinct from, but interlinked with the sovereign cyberspace as well as the national cyberspace at large, as it is mostly run and controlled by private sector corporations. This hybrid character of the sovereign protected cyberspace is what permits and encourages partnerships and collaborations between the public and the private sector. The high degree of individual control over the use of available infrastructure in the domain of the national cyberspace

[80] Id.

is also representative of the need for the construction of legal governance structures in a manner that preserves the 'public core of the internet'[81], and maintains robust linkages with the global Internet at large.

However, this narrow view of the sovereign cyberspace does not imply that the cybersecurity of the rest of the nation, or the broader national cyberspace would be left entirely to the individual. The State must continue to observe and discharge its obligation to guarantee a minimum level of cyber security and data privacy for its citizens, especially on digital platforms conceived, created and operated by it.

NODEs in the National Cyberspace: A Practical Framework

From the description of NODEs in the Whitepaper, it is unclear whether NODEs that are utilised for the delivery of public services would be treated as a part of CII, or a 'protected system' within the meaning of section 70 of the Information Technology Act, 2000.

However, given the high volume of personal and sensitive personal data that is likely to be captured by the NODEs, it is imperative to accord a very high priority to ensuring the overall security of the delivery platforms as well as the security of private information that citizens may share on them.

We envision the NODE architecture as an overlay of interconnected systems and databases that cuts across the three layers of the sovereign cyberspace, sovereign protected cyberspace and national cyberspace. The NODE architecture should be geared towards establishing connections and networks that can be leveraged for improved governance, delivery of public services as well as grievance redressal in case of security breaches.

In doing so, it may be useful to consult practical frameworks for developing the digital ecosystem. One such framework is developed by Omar Valdez-De-Leon[82], and can

[81] Id. at p.35, See also Global Commission on Stability of Cyberspace, 'Advancing Cyberstability Final Report' (November 2019) <https://cyberstability.org/wp-content/uploads/2019/11/GCSC-Final-Report - November-2019.pdf> accessed on 28 May 2020.

also be used as a 'checklist' when developing a strategy for digital ecosystems. He defines digital ecosystems as, "loose networks of interacting organisations that are digitally connected and enabled by modularity, and that affect and are affected by each other's offerings".[83] The interconnections between interacting organisations are characterized by modularity, signifying the absence of management by a hierarchical authority[84].

The most salient takeaway from his definition is the feature of **'modularity'**[85] in a digital ecosystem, which represents an absence of hierarchy in the governance structure. In our understanding, digital ecosystems have been conceived under the NODE Whitepaper as a means of delivery of public services to the citizens from the Government (State or Central), with aid and assistance of the private sector.

Thus, the Government, private sector as well as citizens who choose to join platforms conceived and constructed as NODEs must be treated in law as equal partners that create and sustain the digital ecosystem, and contribute to its smooth functioning and different aspects of governance. Citizens must not be treated as mere subjects in a hierarchical regime where the terms of service are decided solely by Government authorities who may be exempted[86] from the requirement of adherence to best practices in cyber security and data privacy.

---

[82] Omar Valdez-De-Leon, 'How to develop a Digital Ecosystem: A Practical Framework' (August 2019) 9(8) Technology and Innovation Management Review at pp. 43-54 <https://timreview.ca/sites/default/files/article_PDF/TIMReview_August2019-%20Final%20-%20D.pdf> accessed on 28 May 2020.

[83] Id. at pg 44.

[84] Ibid. See also Michael Jacobides, 'Designing Digital Ecosystems' in M. Jacobides, et.al. Platforms and Ecosystems: Enabling the Digital Economy (Briefing Paper, World Economic Forum) <http://www3.weforum.org/docs/WEF_Digital_Platforms_and_Ecosystems_2019.pdf> at pp. 13-19 accessed on 28 May 2020.

[85] According to Omar Valdez-De-Leon, they key building blocks of the ecosystem are openness, modularity and quality. Openness means that the platform allows access to platform resources (via APIs, for example) enabling ecosystem participants to develop their own use cases. Modularity is a key driver to developing digital ecosystems as it enables different organizations to build complementary products or services. Quality means features that enable high availability, reliability, and security, which can be highly valued by ecosystem participants. This in turn will help attract other participants to the ecosystem; Omar Valdez-De-Leon, (n 82).

[86] See for example, Clause 35 of the Personal Data Protection Bill, 2019 (n 16).

Valdez-De-Leon identifies **three key constituent elements** of digital ecosystems – namely, platform, market expectations and network effects. The **platform** is the key building block of the ecosystem; the enabler upon which ecosystem partners can build their products or services[87]. It also supports the two other elements – network effects and market expectations.

Network effects concerns the self-perpetuating cycle of ecosystem participation and user enrolment. More participants and products or services on the platform lead to more end-users attracted to it, and vice versa – the emphasis is on creating and sharing value across the ecosystem[88].

Market expectation is related to how prospective users perceive an ecosystem in terms of its potential to become widespread in the long term – it is based not on the network's current scale, but rather the number of users with whom they expect to be able to interact with in the future[89]. Thus, we can observe the need to develop a cyclical relationship between network effects and market expectations, to create a digital ecosystem that is self-perpetuating and self-sustaining.

Valdez-De-Leon identifies six **enablers** that can be utilized to develop and activate these constituent elements[90]. These enablers are:

a) APIs as the basic building blocks in the digital ecosystem;

b) Communities of participants who are able to develop products and services based on platform resources;

c) Spearhead products or services that drive the ecosystem development;

d) Support functions for ecosystem participants;

[87] Omar Valdez-De-Leon (n 82) at pg 47.
[88] Id. at pp. 47-48.
[89] Id. at p. 48.
[90] Id. at pp. 49-50.

e) Revenue model that incentivizes participants to join the ecosystem at an early adoption stage, but is also aligned with the realities of current markets and is also fair to all partners involved; and

f) Governance based on a set of clearly defined rules that enable transparency.

The key elements along with enablers of the digital ecosystem are represented thus:

(Figure 2)

An ideal legal framework for NODEs should design administrative processes for NODEs in a manner that enables the creation of a self-sustaining cyclical relationship between market expectation and network effects of the basic platform. In order to foster productive and sustainable partnerships across the public, and private sectors and civil society, **free, meaningful and informed consent**[91] of individuals must be placed at the core of the technological architecture of NODEs. This will give an impetus to market expectations, drive network effects and cultivate communities to enable digital ecosystems that are accessible, accountable, transparent and sustainable.

C. Accountability through strong governance structures

The NODE Whitepaper does not contemplate a primary legislation that will back the entire ecosystem. Therefore, it becomes imperative that governance structures within the architecture are established, both at the central level, where core principles and guidelines are determined for the entire ecosystem, and at the digital platform level,

[91] Please refer to the discussion on consent frameworks in section 2(B) above.

where governance structures are built specific to the sector in which the NODE is operating. In the absence of a data protection law, special regulatory mechanisms for the protection and enforcement of data privacy of citizens need to be established too, in line with the Data Protection Authority of India as proposed by the PDPB 2019[92].

For individual NODEs it will be prudent to rely on existing sectoral regulators/ government departments such as the Reserve Bank of India and the Ministry of Finance for the finance sector and Telecom Regulatory Authority of India and the Department of Telecommunications for the telecom sector.

The regulatory body responsible for each NODE must enjoy a reasonable level of independence in its operation and should not be wholly dependent on the State for its appointment, management, and functioning.

Clear rules of governance which lay down how different stakeholders interact with each other and how their grievances will be addressed at every layer will be an important aspect to consider while building a NODE[93]. In a study on the development of smart cities in developing countries, Tan and Taeihagh[94] found that success in massive technological projects like smart cities[95] can only be realised when concurrent socioeconomic, human, legal, and regulatory reforms are instituted. They argue that for the development of such projects, governments must, inter alia, fulfil the basic infrastructure needs of citizens, construct clear regulatory frameworks to mitigate the technological risks involved, and ensure digital inclusivity. One of the key areas which drive the development of smart cities as identified by the authors is building a strong regulatory environment which fosters confidence and trust of citizens and investors. They argue that having strong and transparent regulatory institutions will enable the government to build the trust of citizens and investors alike. Additionally, as barriers to

[92] Please refer to Sec. 41 of the Personal Data Protection Bill 2019 (n 16).
[93] Reference made to Omar Valdez-De-Leon (n 82).
[94] Tan and Taeihagh, 'Smart City Governance in Developing Countries: A Systematic Literature Review' Sustainability 2020, 12(3), 899 (MDPI) <https://www.mdpi.com/2071-1050/12/3/899> accessed 28 May 2020.
[95] Id. It is essential to draw a link between smart cities and complex data driven models of e-governance like the NODE ecosystem. The relationship between the two is that the main goals for both architectures is - improving government efficacy in public service delivery and promoting inclusive governance.

smart city development, Tan and Taeihagh identify the lack of a central authority to steer the development process and missing governance frameworks to be key factors. They also identify the example of lack of regulatory safeguards for the breach of data privacy and security as a major impediment to smart city development. Adopting lessons from such studies, it is essential that NODEs are supported by a transparent governance and regulatory system for adequate enforcement and protection of citizen rights.

The OECD Recommendations on Digital Government provides guidance on the establishment of effective organisational and governance frameworks within and across levels of government for building an effective e-government strategy.

CCG recommendations

- As held by the Supreme Court, in multiple decisions on the arbitrariness of Government contracts, it is essential that transparency measures such as public auctions, criteria of selection of private parties, publication of names of all private parties engaged, a database of all private parties which applied/ were considered etc. are incorporated in legal and policy frameworks for NODEs, in order to ensure that processes for executing these systems are not arbitrary in nature.

- According to global best practices, openness, transparency, inclusiveness and accountability in government processes are considered as first principles on which nations should develop their digital government strategies. Legal and policy frameworks for NODEs must, at each step, demonstrate how it will adhere to these basic principles.

- The NODE architecture must comprehensively consider the cyber security challenges that will arise from the institution of a network which relies on the exchange of personal data between various stakeholders and lay down mechanisms for the mitigation of such risks.

- Strong governance structures which enable Government accountability and operate at both, the central level and for each NODE are essential for building a transparent e-governance ecosystem.

- Specific regulatory agencies need to be identified, or set up where no such body exists for the regulation of NODEs.

- In line with global best practices, the NODE ecosystem must establish a strong regulatory environment which fosters confidence and trust of citizens and investors alike.

4. Community Engagement

The NODE Whitepaper does consider the question of exclusion of citizens from public delivery if digital mechanisms are adopted and replaced by existing models, but does not provide mechanisms to mitigate the risks of such exclusion. Although one of the principles laid down in the NODE Whitepaper is 'inclusiveness', prior experience in public delivery systems in India suggests that digital networks run the risk of becoming focal points of exclusion, if not designed taking into account infrastructural realities of India.

Even though Internet penetration in India has been growing at a steady pace, only about half of India's population enjoys access to Internet services (504 million active users as of November 2019)[96]. Within Internet users in India, there exists a gender divide with male users forming 65% of the entire user base[97]. The gender divide worsens in rural areas, where female users form only 31% of the rural user base[98]. Quality challenges on Internet usage in rural India remain, with connectivity, quality of service and affordability of mobile internet being major challenges[99]. Among Internet users who are 12 years and above, the penetration of the Internet in rural India stands only at 32%[100]. The urban-rural penetration divide along with gender gap in Internet usage, Internet accessibility in India could pose a major challenge to NODEs as a whole.

Since the NODE Whitepaper envisions each NODE to be a digital delivery platform and presumably make use of the public Internet infrastructure as the basic layer, exclusion due to lack of Internet accessibility and infrastructure could be key hurdles. The NODE Whitepaper does not discuss how the paucity of digital infrastructure and Internet accessibility will be overcome and people without access will not be excluded from the benefits of public services, in detail.

---

[96] IAMAI and Nielson, 'Digital in India 2019: Round 2 Report' <https://cms.iamai.in/Content/ResearchPapers/2286f4d7-424f-4bde-be88-6415fe5021d5.pdf> accessed 28 May 2020.
[97] Id.
[98] Id.
[99] Id.
[100] Id.

A. Aadhaar and exclusion

Studies have shown that due to poor infrastructure and design in some situations, especially where the poor heavily rely on government schemes like the Public Distribution System ("PDS") for ration delivery, the Aadhaar project has led to exclusion of benefits despite reducing leakages[101]. A recent National Bureau of Economic Research working paper[102] found that Aadhaar authentication falsely rejected genuine PDS beneficiaries either due to an exclusion error or because of no links between their Aadhaar and ration cards[103]. Reports have pointed to issues with biometric authentication services using Aadhaar, which have resulted in exclusion of genuine beneficiaries of Government services[104]. It is important to point out that lessons from the implementation of the Aadhaar scheme must be considered by MeitY while formulating the strategy on the NODE ecosystem and alternative methods to digital delivery of services should be provided at each stage to avoid exclusion of genuine beneficiaries.

B. Citizen engagement and digital literacy

Since the main goal of any NODE will be to deliver public services to the citizens, it will be imperative to engage with citizens at each stage of policy formulation and implementation to assure that government intervention results in benefits to the public at large.

Tan and Taeihagh, in their study on smart cities and challenges for developing nations[105], have found that active citizen engagement must include embracing the

[101] Jahnavi Sen, 'New Study Backs Reports That Aadhaar-PDS Link in Jharkhand Led to Exclusions' (The Wire, 21 Feb 2020) <https://thewire.in/rights/aadhaar-pds-ration-cards-jharkhand-jpal> accessed 28 May 2020.

[102] Karthik Muralidharan et al. 'Identity verification standards in welfare programs: Experimental evidence from India' National Bureau of Economic Research, Working Paper Series, Number 26744 <https://www.nber.org/papers/w26744.pdf> accessed 28 May 2020.

[103] Praveen Chakravarty, 'Aadhaar, no standout performer in welfare delivery' The Hindu (28 February 2020) <https://www.thehindu.com/opinion/op-ed/aadhaar-no-standout-performer-in-welfare-delivery/article 30935353.ece> accessed 28 May 2020.

[104] Kunal Purohit, 'In India's Second Poorest State, Govt Efforts To Curb Hunger Are Failing' (IndiaSpend, 7 December 2019) <https://www.indiaspend.com/in-indias-second-poorest-state-govt-efforts-to-curb-hunger-are-failing/> accessed 28 May 2020.

[105] Tan and Taeihagh (n 94).

notions of citizen empowerment, digital inclusion, collaborative governance, behavioural change to ensure that objectives of developmental projects are realised. They argue that the lack of citizen participation or public involvement presents a major challenge for governments in technologically dependent projects[106] in developing countries. Another reason a model like the NODE ecosystem could result in exclusion is technological illiteracy and knowledge deficit among citizens. Low levels of digital literacy impact the uptake of digital solutions, and may affect the overall success of an e-governance model[107]. Universal digital literacy and accessible digital resources are also key vision areas[108] of the Government's Digital India initiative, and must be a key feature of the NODE strategy as well.

C. International Best Practices

The UN e-Gov Survey notes some key findings on challenges of exclusion through e-governance projects. It notes that though digital technologies offer opportunities of inclusion, existing digital divides due to inequities in the larger population could result in exclusion of individuals who do enjoy access to modern digital infrastructure. Hence, it becomes imperative that Governments ensure that e-governance projects do not result in exclusion of the less privileged[109]. The UN e-Gov Survey finds that in order to reap the full rewards of e-governance projects, access to high speed broadband and grater bandwidth become necessary components[110]. To ensure inclusion, recognition of digital divides on the basis of income, gender, and societal realities becomes important and countries which run a 'digital first' policy without taking into consideration digital infrastructure realities may face risks of social exclusion[111]. The UN e-Gov Survey places emphasis on digital literacy, not just among the population but also civil servants for building meaningful digital delivery services. Another finding which is of key importance from the UN e-Gov Survey is the existence of a strong correlation between

[106] Id. In their study they focus on smart cities projects as technologically driven public initiatives
[107] Based on findings of Tan and Taeihagh (n 94).
[108] Digital India, 'Vision and Vision Areas' <https://www.digitalindia.gov.in/content/vision-and-vision-areas> accessed 28 May 2020.
[109] UN E-Government Survey 2018 (n 8) at Chapter 2.
[110] Id.
[111] Id.

digital and social exclusion. Vulnerable groups, such as people with disabilities find it increasingly hard to access digital public services, due to accessibility issues. The design of the NODE architecture must keep the socio-economic reality of India in context while building a digital first framework. Mitigation strategies around challenges such as digital infrastructure, literacy, digital divides, and accessibility issues of the vulnerable population should form the core part of the design ethos of NODEs.

CCG recommendations

- Policy frameworks for NODEs need to focus on the current state of digital infrastructure in India and build alternate strategies, so that such digital projects like the NODE architecture do not result in exclusion of genuine beneficiaries.

- Lessons from exclusion in the Aadhaar system should be considered and future strategies must be built to address known challenges.

- Since the prime objective of building the NODE architecture is to ensure efficient delivery of public services using digital platforms, citizen engagement becomes imperative to the success of such a project. The Government must collaborate with the public at each stage to ascertain the best strategy for developing NODEs.

- Learning from global best practices and studies – which state that digital first projects which don't take into account the socio-economic fabric of a nation and run the risk of social exclusion – must be considered by MeitY and mitigation strategies should be developed against exclusion.