RESPONSE TO THE

CONSULTATION WHITEPAPER ON THE STRATEGY FOR NATIONAL OPEN DIGITAL ECOSYSTEMS (NODE)

March 2020 | *Issue No. 103*

ESYA centre

ABOUT THE ESYA CENTRE

The Esya Centre's mission is to generate empirical research and inform thought leadership to catalyse new policy constructs for the future. It simultaneously aims to build institutional capacities for generating ideas which enjoin the triad of people, innovation and value, consequently helping reimagine the public policy discourse in India and building decision-making capacities within government.

Esya invests in ideas and encourages thought leadership through collaboration. This involves curation of niche and cutting-edge research, and partnerships with people, networks and platforms. Moreover, it prioritises multi-disciplinary research to engender "research clusters", through which practitioners and researchers collaborate.

RESPONSE TO THE
CONSULTATION WHITEPAPER ON THE STRATEGY FOR NATIONAL OPEN DIGITAL ECOSYSTEMS (NODE)

We at the Esya Centre greatly appreciate the opportunity given to us by the Ministry of Electronics and Information Technology (**MEITy**) to respond to the consultation whitepaper on the 'Strategy for National Open Digital Ecosystems (NODE)' (**Whitepaper**), which solicits public comments for developing a comprehensive national strategy on NODE.

We appreciate that MEITy has identified design principles to develop a framework for digital governance through the Whitepaper, and that it has also identified key concerns that would need to be accounted for in developing the NODE framework. In answering the questions posed in the Whitepaper, we have focused our feedback on those relating to design principles, governance, and the potential risks of open digital ecosystems. We have approached this analysis from a broad, techno-legal perspective, and focusing on the rights and obligations of various stakeholders.

Part I of this response will provide a brief snapshot of our recommendations under the relevant questions, which will thereafter be explored in detail in **Part II**. We hope that these discussions will prove instructive in a larger discourse about digital governance in India.

PART I

QUESTION (PER THE WHITEPAPER)	COMMENTS
Q1. 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.	**Section 4.1** of the Whitepaper outlines the principles for the design of delivery platforms. We recommend that **Principle 4** (on security and privacy) is modified to include a focus on cybersecurity, given the potential implications of security lapses in critical infrastructure. **Section 4.2** of the Whitepaper outlines the principles for transparent governance. We recommend that **Principle 10** (on adopting a suitable financing model) is modified to include transparency and disclosure on the sources and use of funds. This is essential especially since NODEs will involve public-private participation and funding, and such disclosures are essential to develop trust, maintain accountability, and increase participation. **Section 4.3** of the Whitepaper outlines the principles for a vibrant community. We recommend that **Principle 11** (on ensuring inclusiveness) is modified to include a focus on building awareness and education regarding digital services, their use and associated risks. This would ensure that services provided through NODEs are inclusive and help bridge existing digital divides.
Q5. DO NODES ACROSS SECTORS REQUIRE COMMON GOVERNANCE FRAMEWORKS AND REGULATORY/ ADVISORY INSTITUTIONS TO UPHOLD THESE? OR IS IT SUFFICIENT FOR EACH NODE TO HAVE AN INDIVIDUAL GOVERNANCE CONSTRUCT? IF A COMMON FRAMEWORK IS REQUIRED, PLEASE ELABORATE THE RELEVANT THEMES/ TOPICS E.G. FINANCING, PROCUREMENT, DATA SHARING.	We recommend that NODEs have individual as well as shared governance frameworks, in order to maintain policy coherence, standardise thresholds, monitor and evaluate implementation on cross-sectoral issues, and offer effective redressal mechanisms. Key themes for the common frameworks include: (a) Data governance (b) Cybersecurity (c) Financing (d) Overall governance
Q7. WHAT ARE SOME POTENTIAL RISKS THAT OPEN DIGITAL ECOSYSTEMS CAN LEAVE CITIZENS VULNERABLE TO, FOR EXAMPLE, RISKS RELATED TO DATA PRIVACY, EXCLUSION, HAVING AGENCY OVER THE USE OF THEIR DATA ETC.? WHAT TYPES OF OVERARCHING GUIDELINES AND/OR REGULATORY FRAMEWORKS ARE REQUIRED TO HELP MITIGATE THEM?	The potential risks that stem from a national digital ecosystem can broadly be classified as those relating to: (a) Cybersecurity and Data Protection (b) Data Privacy and Autonomy (c) Exclusion and Digital Divides Therefore, any overarching guidelines and/or regulatory framework must adopt a bottom-up approach, focused on improving both access and ability of the beneficiaries. This needs to be complimented by a secure and robust security architecture while respecting the fundamental right to privacy and providing for adequate control over personal data.

Q14. HOW WOULD YOU LIKE TO ENGAGE FURTHER (E.G. INDIVIDUAL CONSULTATIONS, WORKSHOPS, ETC.) AS WE BUILD THE STRATEGY FOR NODE?

We greatly appreciate the opportunity to respond to the Whitepaper and would be happy to engage further in developing this framework through written submissions on targeted issues, workshops, consultations, and other methods of engagement that MEITy may formulate.

PART II

Q1. 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.

Section 4.1 of the Whitepaper outlines the principles for the design of delivery platforms. While the principles identified are necessary in this regard, we urge that **Principle 4** (on security and privacy) is modified to include a focus on cybersecurity, and the monitoring of data flows within each NODE. Building strong security and monitoring mechanisms into the design of the NODE frameworks is essential to prevent lapses in the security of NODEs and other critical infrastructure.[1] This has been discussed in further detail in our responses to Q5 and Q7 below.

Section 4.2 of the Whitepaper outlines the principles for transparent governance. While the principles identified are necessary in this regard, we urge that **Principle 10** (on adopting a suitable financing model) is modified to include transparency in terms of funding, and to require regular, periodic publication of financial contributors to each NODE. Transparency and disclosure requirements are built into corporate governance, in part, to enable interested stakeholders to monitor performance, make informed decisions on investment, and improve management.[2] Financial transparency and reporting standards have been successfully adopted in governance models as well[3]. Given that the NODE framework anticipates and encourages public-private participation and funding, such disclosures are essential to develop trust, maintain accountability, and increase participation.

Section 4.3 of the Whitepaper outlines the principles for transparent governance. While the principles identified are necessary in this regard, we urge that **Principle 11** (on ensuring inclusiveness) is modified to include a focus on building awareness and education regarding digital services, their use and associated risks. Such measures would be crucial in ensuring that the creation of a digital ecosystem does not result in the widening of existing digital divides in Indian society.[4] In addition to on-boarding and platform adoption, which are mentioned in the Whitepaper, attention needs to be paid to skill development that allows for effective and secure usage.

[1] *United Nations e-Government Survey 2018, Gearing e-Government to support Transformation towards Sustainable and Resilient Societies, pp. 76-77, accessible at: https://www.un.org/development/desa/publications/2018-un-e-government-survey.html.*

[2] *Chris S Armstrong, Wayne R. Guay, Hamid Mehran, and Joseph Peter Weber, The Role of Financial Reporting and Transparency in Corporate Governance (2016), Economic Policy Review, Issue Aug, pp. 109, accessible at: https://ssrn.com/abstract=2828077; see also Reserve Bank of India, Master Circular - Disclosure in Financial Statements - 'Notes to Accounts', Introduction, July 1, 2015 accessible at: https://m.rbi.org.in/Scripts/BS_ViewMasterCirculars.aspx?Id=9906&Mode=0.*

[3] *United Nations e-Government Survey 2018, Gearing e-Government to support Transformation towards Sustainable and Resilient Societies, p. 6, accessible at: https://www.un.org/development/desa/publications/2018-un-e-government-survey.html.*

[4] *YS Sipre, Bridging Digital Divides in India: Some factors and initiatives, International Journal of Digital Library Services, Vol. 7, April - June, 2017, Issue - 2, accessible at: http://www.ijodls.in/uploads/3/6/0/3/3603729/5ijodls217.pdf.*

Q5. DO NODES ACROSS SECTORS REQUIRE COMMON GOVERNANCE FRAMEWORKS AND REGULATORY/ ADVISORY INSTITUTIONS TO UPHOLD THESE? OR IS IT SUFFICIENT FOR EACH NODE TO HAVE AN INDIVIDUAL GOVERNANCE CONSTRUCT? IF A COMMON FRAMEWORK IS REQUIRED, PLEASE ELABORATE THE RELEVANT THEMES/ TOPICS E.G. FINANCING, PROCUREMENT, DATA SHARING.

We recommend that NODEs have individual as well as shared governance frameworks. While individual NODEs would deal with specific areas, there are overarching issues (such as cybersecurity and data protection, for example) that each NODE would have to conform with. Having common regulatory/advisory institutions can help maintain policy coherence, standardise thresholds, monitor and evaluate implementation on cross-sectoral issues, and offer effective redressal mechanisms.[5] This is especially important given that the framework envisioned in the Whitepaper requires coordination and dialogue between different stakeholders and NODEs.

Shared governance frameworks may be instituted by setting up relevant institutional/advisory bodies. However, since this could be expensive, time-consuming, and potentially create regulatory conflict, we recommend that existing ministries and agencies are tasked with overseeing specific areas in which they have expertise. For instance, the Data Protection Authority (DPA) (proposed under the Personal Data Protection Bill, 2019 (PDP Bill)[6]) could oversee data governance, the Ministry of Finance could govern financing, and MEITy could be tasked with cybersecurity. Each NODE could also have a committee for each of these shared governance frameworks, which could serve as points of contact for the frameworks and aid in coordination amongst various NODES and departments.

However, any new regulatory frameworks and guidelines would have to be harmonised with existing architecture and guidelines framed for e-governance. These include, for instance, the India Enterprise Architecture framework, which comprises architecture reference models which are meant to aid in developing enterprise architecture[7], various e-governance standards, ranging from the adoption of open source software in e-governance, security guidelines for the use of biometrics, etc.[8]

Key themes under common governance frameworks for NODEs include:

(a) ***Data governance***

Data in multiple forms comprises the core of the NODE framework and e-governance in general. The Whitepaper recognises its importance in Principle 8 of Section 4.2, when it identifies transparent data governance as key to effective governance of the NODE framework. NODEs will comprise mixed datasets consisting of both the personal data (data that can be used to identify a person[9]), as well as non-personal data (comprising aggregate/ anonymised datasets, usage patterns of communities, etc.). Per the PDP Bill, it is likely that mixed datasets will be treated as personal data[10]. This is

[5] OECD Digital Government Studies, Digital Government Review of Brazil, Towards the Digital Transformation of the Public Sector, November 2018, pp. 18-19, accessible at: https://www.oecd-ilibrary.org/governance/digital-government-review-of-brazil_9789264307636-en.

[6] Clause 41, Personal Data Protection Bill, 2019.

[7] The eight reference models are Business, Application, Data, Technology, Performance, Security, Integration and Architecture Governance. See generally India Enterprise Architecture Framework, October 2018, accessible at: http://egovstandards.gov.in/sites/default/files/IndEA%20Framework%201.0.pdf.

[8] See generally STQC Directorate, MEITy, e-Governance Standards, accessible at: http://egovstandards.gov.in/frameworkinstitutional-mechanism-and-policies.

[9] Clause 2(28), Personal Data Protection Bill, 2019.

[10] Clause 2(28), Personal Data Protection Bill, 2019. Definition of personal data includes 'or any combination of such features with any other information'. This can be interpreted as stating that a combination of features allowing for identification of a person along with other information, whether personal or non-personal i.e. mixed data, will be treated as personal data.

also in line with emerging jurisprudence on mixed and non-personal data in Europe[11]. As a result, any entity involved in the collection, processing, storage and use of data would be required to adhere to provisions of the personal data protection legislation with respect to their datasets. The PDP Bill tasks the DPA with, among other responsibilities, protecting the interests of data principals and ensuring compliance with the data protection legislation[12]. Therefore, the DPA would be well-placed to govern data under the NODE framework.

In this context, it is important to note that there is currently no certainty on the regulation of either personal or non-personal data in India. The PDP Bill has not yet been passed and is currently before a Select Committee of Parliament, and a Committee of Experts has been formulated to develop principles for the governance of non-personal data[13]. The eventual laws governing both these aspects would dictate the treatment of data in the NODE framework and significantly impact governance in this regard. Data protection and related issues have been discussed in further detail in our response to Q7 below.

An aspect of non-personal datasets that is gaining increasing relevance is that of intellectual property. Depending on how intellectual property laws around datasets and non-personal data evolve, and on how the interplay with private companies are framed in each of the NODEs, there are likely to be intersections with copyright and trade secret laws.

(b) Cybersecurity

A key area to consider when developing e-governance frameworks is cybersecurity. Poor cybersecurity can expose users and organisations to risks, expose vulnerable or private data, significantly hinder the democratic process, and more generally create distrust in the digital economy and impact adoption of new technologies[14]. The nature and volume of data being generated, stored and processed in the operation of a digital ecosystem makes it a prime target for malicious attacks as well as a source of potential leaks of user information. Increasingly, state run public delivery systems are being targeted by denial of service attacks, distributed denial of service attacks as well as ransomware attacks which have resulted in millions of dollars of losses in just the past year[15]. Cybersecurity has also been compromised to achieve political ends – for instance, the 2007 attack on Estonia's digital ecosystem crippled the country and various sectors such as schools, banks, internet service providers, and media channels[16]. While there

[11] European Commission, Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union, May 29, 2019, Retrieved from EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019DC0250&from=EN; Patrick Breyer v Bundesrepublik Deutschland, C-582/14 (Court of Justice of the European Union October 19, 2016).

[12] Clause 49, Personal Data Protection Bill, 2019.

[13] PRS Legislative Research, The Personal Data Protection Bill, 2019, accessible at: https://www.prsindia.org/billtrack/personal-data-protection-bill-2019; MEITy, Office Memorandum, Constitution of a Committee of Experts to Deliberate on Data Governance Framework, September 13, 2019, accessible at:, https://MEITy.gov.in/writereaddata/files/constitution_of_committee_of_experts_to_deliberate_on_data_governance_framework.pdf.

[14] Internet Governance Forum 2017, Best Practice forum on Cybersecurity, pp. 9-10, accessible at: https://www.intgovforum.org/multilingual/index.php?q=filedepot_download/4904/1017.

[15] See, for example, Robert Muggah and Marc Goodman , Cities are easy prey for cybercriminals. Here's how they can fight back, World Economic Forum, September 20, 2019, available at: https://www.weforum.org/agenda/2019/09/our-cities-are-increasingly-vulnerable-to-cyberattacks-heres-how-they-can-fight-back/.

[16] Jaan Priisalu and Rain Ottis, Personal Control of privacy and data: Estonian experience, p. 445, Health and Technology 2017, accessible at: https://link.springer.com/article/10.1007/s12553-017-0195-1.

are currently some standards on cybersecurity in limited contexts in India[17], there is a pressing need for comprehensive regulation in this regard.

This is especially important to achieve India's e-governance objectives, as the success of such initiatives are highly dependent on ensuring trust and security in e-governance systems. It is therefore concerning that the Whitepaper has not addressed the issue of cybersecurity in detail. Even though India has built the foundations of its digital security architecture and featured in the top quarter of countries in the Global Cybersecurity Index in 2018[18], the operationalisation of open digital ecosystems without a clearly formulated cybersecurity legislation is a significant risk. In comparison, nearly all European nations have adopted cybersecurity legislations and regulations, and these form the basis of digital ecosystems that inspire trust and confidence among citizens[19].

An effective cybersecurity framework would need to institute systems whereby security vulnerabilities are proactively found and fixed, and include mechanisms to address concerns and plug leaks exposed by researchers.[20] In this context, it is also important that researchers who seek out vulnerabilities in public interest are protected from liability, as they play an important role in discovering security leaks[21]. This would also go a long way in developing the trust required for any system to effectively function on a national scale and foster participation. Other measures that can be taken to enhance cybersecurity are covered in more detail in our response to Q7 below.

Since internet governance and administration of information technology and cyber laws fall under the mandate of MEITy[22], it could be tasked with framing adequate cybersecurity regulations for e-governance.

(c) *Financing*

In **Principle 10**, the Whitepaper recognises the importance of adopting sustainable financing models in each NODE and envisages a combination of public and private funding. While this approach is necessary, it is essential to situate such a framework in transparency, accountability, and ethical leadership. A key method to achieve these aims is to disclose sources and amounts of funding, and budget execution for each NODE. This would also aid in monitoring usage of funds and increase public trust and participation[23]. Fiscal transparency on tax use has been seen to be very effective in maximising efficiency in the Republic of Korea, and releasing such information with supporting materials to understand key indicators

[17] See for instance, MEITy, Security Guidelines for use of Biometric Technology in e-Governance Projects, accessible at: http://egovstandards.gov.in/sites/default/files/Security%20Guidelines%20for%20use%20of%20Biometric%20Technology%20in%20e-Governance%20Projects.pdf.

[18] International Telecommunication Union, Global Cybersecurity Index Report 2018, available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

[19] International Telecommunication Union, Global Cybersecurity Index Report 2018, available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

[20] Internet Governance Forum 2017, Best Practice Forum on Cybersecurity, p. 24, accessible at: https://www.intgovforum.org/multilingual/index.php?q=filedepot_download/4904/1017.

[21] Internet Governance Forum 2017, Best Practice Forum on Cybersecurity, p. 25, accessible at: https://www.intgovforum.org/multilingual/index.php?q=filedepot_download/4904/1017.

[22] MEITy, Functions of Ministry of Electronics and Information Technology, accessible at: https://MEITy.gov.in/about-MEITy/functions-of-MEITy.

[23] United Nations e-Government Survey 2018, Gearing e-Government to support Transformation towards Sustainable and Resilient Societies, p. 6, accessible at: https://www.un.org/development/desa/publications/2018-un-e-government-survey.html.

has aided in increasing participation[24]. Building similar requirements into the regulatory framework on financing for NODEs would be key to maximising trust and accountability.

(d) Competition and Innovation

The creation of open digital ecosystems can lead to the creation of a new marketplace wherein firms would be encouraged to compete with each other to offer better delivery of services, while benefiting from the insights provided by the large volumes of data that is generated. Therefore, a key objective that any policy framework should achieve is ensuring competitiveness in the market. It is well established that competitive markets have numerous advantages in terms of fostering innovation, promoting efficiency, increasing choice and availability as well as lower prices[25]. Conversely, a lack of competition impedes inclusion, creates stagnation, disincentivises investment and innovation[26].

The digital services ecosystem faces various impediments which may hinder competition. These may broadly be classified into two types. The first are structural impediments, which relate to the nature and structure of the market, such as the network effect, high initial sunk costs and economies of scale. The second are strategic impediments, which arise from the behaviour of firms in the market, such as refusal to share data, creation of silos as well as limiting access to communication systems[27]. In addition, large players such as Amazon or Google, with access to customer data and preferences from their routine business may enjoy a distinct advantage in service targeting and delivery provided through the NODEs[28]. Using the digital financial services sector as a proxy, we can see the emergence of dominant players such as mPesa in Kenya bKash in Bangladesh and even the National Payments Corporation of India as examples of the proclivity of the digital services ecosystem to favour market concentration[29].

In light of the above, a framework policy for open digital ecosystems must be able to ensure ease of market entry, a level playing field in the relevant market, and prevention of abuse of dominant position or the creation of anti-competitive agreements through mergers and acquisitions or cartelisation[30]. While most of these matters fall within the ambit of the Competition Act, 2002 and consequently will be regulated by the Competition Commission of India, a common anti-competitive policy must address issues relating to licence requirements for new entities, data sharing

24 United Nations e-Government Survey 2018, Gearing e-Government to support Transformation towards Sustainable and Resilient Societies, p. 6, accessible at: https://www.un.org/development/desa/publications/2018-un-e-government-survey.html.

25 di Castri, Simone and Plaitakis, Ariadne, Getting Financial Inclusion Policies Right in the Digital Era: Focus on Competition and Innovation as Policy Objectives, p.1, October 1, 2018. Available at: https://ssrn.com/abstract=3267563 or http://dx.doi.org/10.2139/ssrn.3267563.

26 United Nations Conference on Trade and Development, Secretariat Note on the Benefit of Competition Policy for Consumers.

27 Matthew Sourosorian and Ariande Plaitakis, Fair Play: Ensuring Competition in Digital Financial Services, p.4, Working Paper, CGAP, World Bank, 2019, accessible at: https://www.cgap.org/sites/default/files/publications/2019_11_Working_Paper_FairPlay.pdf.

28 Justus Haucap & Ulrich Heimeshoff, Google, Facebook, Amazon, eBay: Is the Internet driving competition or market monopolization, International Economics and Economic Policy, February 2014, accessible at: https://www.researchgate.net/publication/263231006_Google_Facebook_Amazon_eBay_Is_the_Internet_driving_competition_or_market_monopolization.

29 Sector Statistics Report of the Communications Authority of Kenya, 2018 and Joep Roest, 2017 Global Findex: Behind the Numbers on Bangladesh, CGAP blog post, 24 July 2018, accessible at: https://www.cgap.org/blog/2017-global-findex-behind-numbers-bangladesh.

30 Matthew Sourosorian and Ariande Plaitakis, Fair Play: Ensuring Competition in Digital Financial Services, p.7, Working Paper, CGAP, World Bank, 2019, accessible at: https://www.cgap.org/sites/default/files/publications/2019_11_Working_Paper_FairPlay.pdf.

practices and mechanisms for price disclosure and discovery. In addition, it must ensure all entities have equal and fair access to communication channels and payments and clearing systems. These objectives must also be balanced with the goal of fostering innovation and allowing for the creation of new and improved services by offering relevant protection through intellectual property rights. Therefore, a system of proportionate regulation[31], wherein nascent entities can adapt and formulate new technology solutions while systemically important entities are subject to closer control and scrutiny could be adopted.

(e) Overall governance

Coordination and policy coherence can play an important role in driving e-government initiatives[32]. To this end, it would be useful to have a nodal agency in charge of e-governance for NODEs in India, so that common standards on transparency and accountability can be established and monitored. For instance, in Brazil, the System for the Administration of Information Technologies Resources (SISP) acts as the coordinating agency across different sectors of the executive[33]. This role could potentially be fulfilled by MEITy's National e-Governance Division (**NeGD**), which is currently tasked with supporting MEITy in managing and implementing various e-governance projects and initiatives at the state and central levels[34]. However, for effective e-governance, the division would have to develop capabilities beyond technical expertise. Long-term effective governance depends on creating trustworthy, accountable, inclusive, and effective frameworks for service delivery[35]. Transparency, accountability, and inclusiveness are particularly important to garner trust for such frameworks [36].

Q7. WHAT ARE SOME POTENTIAL RISKS THAT OPEN DIGITAL ECOSYSTEMS CAN LEAVE CITIZENS VULNERABLE TO, FOR EXAMPLE, RISKS RELATED TO DATA PRIVACY, EXCLUSION, HAVING AGENCY OVER THE USE OF THEIR DATA ETC.? WHAT TYPES OF OVERARCHING GUIDELINES AND/OR REGULATORY FRAMEWORKS ARE REQUIRED TO HELP MITIGATE THEM?

Examples from various nations across the world have illustrated the immense potential digital ecosystems possess in furthering efficiency, reducing leakages, and ensuring on-time and targeted delivery of services[37]. The Whitepaper itself lists out several positive instances of the use of GovTech 3.0 or NODEs, such as the UPI Platform and GSTN[38], to show how such systems may be successfully implemented in India.

Nevertheless, collecting, storing and processing such large sums of data, including the personal data of citizens, is fraught with various risks that must be guarded against. Here, we seek to identify potential harms which may arise in the course

[31] As recommended by the Financial Sector Legislative Reforms Commission Working Group on Payments.
[32] United Nations e-Government Survey 2018, Gearing e-Government to support Transformation towards Sustainable and Resilient Societies, p. 8, accessible at: https://www.un.org/development/desa/publications/2018-un-e-government-survey.html.
[33] OECD Digital Government Studies, Digital Government Review of Brazil, Towards the Digital Transformation of the Public Sector, November 2018, p. 19, accessible at: https://www.oecd-ilibrary.org/governance/digital-government-review-of-brazil_9789264307636-en.
[34] National e-Governance Division, About National e-Governance Division, accessible at: https://negd.gov.in/node/67.
[35] United Nations e-Government Survey 2018, Gearing e-Government to support Transformation towards Sustainable and Resilient Societies, pp. 5-6, accessible at: https://www.un.org/development/desa/publications/2018-un-e-government-survey.html.
[36] United Nations e-Government Survey 2018, Gearing e-Government to support Transformation towards Sustainable and Resilient Societies, p. 5, accessible at: https://www.un.org/development/desa/publications/2018-un-e-government-survey.html.
[37] UNDESA, Compendium of Innovative Practices in Public Governance and Administration for Sustainable Development, 2016, accessible at: https://publicadministration.un.org/publications/content/PDFs/Compendium%20Public%20Governance%20and%20Administration%20for%20Sustainable%20Development.pdf.
[38] MEITy, Consultation Paper on Strategy for National Open Digital Ecosystems, p5.

of actualising the idea of a NODE by relying on **Principles 4** (ensure security and privacy), **8** (create transparent data governance), and **11** (ensure inclusiveness) enumerated in the Whitepaper. In our analysis, we will rely on parameters from the framework used by the UN E Government Survey, 2018[39]. The Survey identifies and studies best practices in digital governance from across the world and has proved instructive in guiding research for our comments. The following key areas of analysis emerge:

(a) Cybersecurity and data protection

players that are likely to be involved, ensuring system-wide security and proper data management practices can be challenging. This has also previously been an issue - for instance, the e-governance standards (security guidelines) recommend using the Aadhaar framework for biometric data, and not develop separate processes for the same[40]. However, there have been multiple reported authentication issues[41] and data breaches with respect to the Aadhaar database, which have revealed personally identifiable information of users, even if not the core biometric data itself[42].

Many breaches have arisen from middleman misconduct or lax security of private actors, where adequate security measures were not taken by Authentication User Agencies/e-KYC User Agencies or other third parties interacting with the Central Identities Data Repository[43]. These demonstrate how important permissions and the security of supply chain are, apart from the technology itself[44]. They also raise questions about the suitability of biometrics as a method of authentication itself[45]. Existing issues could be exacerbated in the NODE infrastructure, which envisages linkage with private companies via APIs (application programming interfaces) or otherwise. One of the most significant concerns with linking multiple databases with access to many facets of a person's life is that even if the leak of individual pieces of data is not harmful, a combination of such data can be used to infringe on rights and cause harm.

Therefore, an important consideration in maintaining cybersecurity is designing systems to prevent single points of failure by adopting a decentralised approach. The importance of decentralisation to maintain security has also been recognised by the Government[46], and is a principle that must be incorporated into the NODE framework. This would ensure

[39] *United Nations e-Government Survey 2018, Gearing e-Government to support Transformation towards Sustainable and Resilient Societies, pp. 1-23, accessible at: https://www.un.org/development/desa/publications/2018-un-e-government-survey.html.*

[40] *MEITy, Security Guidelines for use of Biometric Technology in e-Governance Projects, June 2017, p. 36, accessible at: http://egovstandards.gov.in/sites/default/files/Security%20Guidelines%20for%20use%20of%20Biometric%20Technology%20in%20e-Governance%20Projects.pdf.*

[41] *Jean Dreze, Done by Aadhar, The Telegraph, September 8, 2018, available at: https://www.telegraphindia.com/opinion/done-by-aadhaar/cid/1467855.*

[42] *Rachna Khaira, Rs 500, 10 minutes, and you have access to billion Aadhaar details, The Tribune, January 4, 2018, accessible at: https://www.tribuneindia.com/news/archive/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details-523361.*

[43] *Zack Whittaker, India's state gas company leaks millions of Aadhaar numbers, Tech Crunch, February 2019, accessible at: https://techcrunch.com/2019/02/18/aadhaar-indane-leak/.*

[44] *Zack Whittaker, A new data leak hits Aadhaar, India's national ID database, ZDNet, March 23, 2018, accessible at: https://www.zdnet.com/article/another-data-leak-hits-india-aadhaar-biometric-database/*

[45] *Aman Sethi and Samarth Bansal, Aadhaar gets new security features, but this is why your data still may not be safe, Hindustan Times, July 19, 2017, accessible at: https://www.hindustantimes.com/india-news/aadhaar-gets-new-security-features-but-this-is-why-your-data-still-may-not-be-safe/story-RoZJAOUXtWZREr4V4M5TvK.html*

[46] *See, for instance, MEITy, Security Guidelines for use of Biometric Technology in e-Governance Projects, June 2017, pp. 15, 18, 25, accessible at: http://egovstandards.gov.in/sites/default/files/Security%20Guidelines%20for%20use%20of%20Biometric%20Technology%20in%20e-Governance%20Projects.pdf; RBI, Policy Paper on Authorisation of New Retail Payment Systems, January 21, 2019, para 9, accessible at: https://www.rbi.org.in/scripts/PublicationReportDetails.aspx?UrlPage=&ID=918.*

that even if there was to be a breach, data loss is minimised. In this context, a strong focus on encryption is also essential to protect the data and communication of individuals and companies and protect against malicious cyberattacks[47].

Suggestions for overarching guidelines and/or regulatory framework

The basis for a cybersecurity regulatory framework should be laid down in the form of a legislation. Such a legislation should allow for the establishment of a minimum standard of behaviour for all entities across the board[48].

To bring about a uniformity in the cybersecurity standards, reporting procedures and best practices, a Government body or agency needs to be created/identified as a regulator. As suggested in our response to Q5, this could be carried out by MEITy's e-Governance Division, provided that requisite skills and expertise are developed. The body should also be tasked with investigating instances of cyberattacks on NODEs, testing security architecture and issuing alerts and warnings. These legal and policy initiatives must be coupled with efforts to create a workforce skilled in cybersecurity and associated issues.

Investments and capacity in cryptographic algorithms must be increased to continuously develop up-to-date encryption protocols. Several nations have experimented with the use of blockchain for encryption while ensuring transparency, traceability and non-repudiation[49].

It is also essential to map the interface of NODEs with their impact on Critical Information Infrastructure (**CII**)[50]. Any vulnerabilities in CII can have massive implications on the functioning of the Government and several other institutions both within and outside the NODE framework.

(b) Data Privacy and Agency

As discussed previously, the functioning of a digital ecosystem is based on the generation, collection and processing of large amounts of data. Since NODEs will comprise mixed datasets, stakeholders in the ecosystem are likely to have to conform with data protection regulations specified in the personal data protection legislation, particularly with regard to explicit consent, purpose limitation, collection limitation, and minimization of data collection[51].

Therefore, and as highlighted by the Whitepaper, it would be important for all players to incorporate privacy by design principles[52]. This would ensure the operation of a NODE is centred around the security and safety

[47] Internet Governance Forum 2018, Best Practice Forum on Cybersecurity: Cybersecurity Culture, Norms and Values, p. 37, accessible at: https://www.intgovforum.org/multilingual/filedepot_download/6764/1437.

[48] United Nations e-Government Survey 2018, Gearing e-Government to support Transformation towards Sustainable and Resilient Societies, p. 72, accessible at: https://www.un.org/development/desa/publications/2018-un-e-government-survey.html

[49] World Bank Group, Cryptocurrencies and Blockchain: Europe and Central Asia Economic Update, May 2018, accessible at: https://openknowledge.worldbank.org/bitstream/handle/10986/29763/9781464812996.pdf.

[50] Section 70A, Information Technology Act, 2000. More information available at: https://nciipc.gov.in/.

[51] https://www.prsindia.org/billtrack/personal-data-protection-bill-2019

[52] Ann Cavoukian, Privacy by Design: the 7 Foundational Principles, accessible at: https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf,

of the citizen providing the data, thereby creating an environment of trust and accountability. This is of utmost importance for the success of digital ecosystems. It is commendable that several of these concerns have been dealt with in the Principles 4 and 8 of the Whitepaper.

However, certain concerns regarding the implementation of these principles remain. The first concern has to do with the operationalisation of a consent framework. India is a nation with a vast population, large portions of which still lack access to telephone and the Internet. In this context, it is difficult to envision how the Electronic Consent Frameworks[53] developed by MEITy will be usable by a sizeable chunk of the population, due to issues of access and literacy. This concern stems from the fact that the consent framework requires the generation of a consent artefact, and validation through digital signatures, both of which appear to be fairly complex procedures. Furthermore, the level of granular control sought to be provided appears to be difficult to capture through simple services such as text messages or IVRS. Equally concerning is the fact the citizens of developing countries are reportedly more susceptible to over-consent, and those from lower income groups are more likely to use apps and or sites with less regard towards privacy permissions and requests[54]. In this regard, it is worthwhile to also consider the extent to which meaningful consent can be exercised to avail of essential services.

The second concern has to do with the lack of a single unique identification mechanism. In Estonia, for example, it is mandatory for each citizen to possess a Digital ID Card which is used to authenticate identity and avail services[55]. While Aadhaar has emerged as a near ubiquitous proof of identity, it suffers from issues such as ghost beneficiaries and frauds[56]. Not only does this make the system susceptible to leakages, it also poses the risk of genuine beneficiaries being excluded from the NODEs. Further, the stipulation for use of Aadhaar to avail such a large gamut of services, including by private players, is likely to fall foul of restrictions laid down by the Supreme Court in Justice *K.S. Puttaswamy and Ors. vs. Union of India*[57]. However, recent developments with regards to tokenisation and Virtual Aadhar are positive steps in the direction of protecting user data and identity. Authentication logs and access reports are also provided over message and texts.[58]

Suggestions for overarching guidelines and/or regulatory framework

While the current data privacy framework is contained in the Information Technology Act, 2000 and relevant rules issued thereafter[59], it would be most sensible for any framework to be designed to be in conformity with the data protection legislation and use the provisions of the PDP Bill as a template. As stated above, this would make the entities liable to implement

53 MEITy, Electronic Consent Framework, Technology Specification, Version 1.1, accessible at: http://dla.gov.in/sites/default/files/pdf/MEITy-Consent-Tech-Framework%20 v1.1.pdf.
54 McGowan, Vora, , Homer, and Dolan., Personal data empowerment: restoring power to the people in a digital age, Pathways for Prosperity Commission Background Paper Series; no. 11. Oxford, United Kingdom, 2018, accessible at: https://pathwayscommission.bsg.ox.ac.uk/sites/default/files/2018-11/personal_data_empowerment.pdf.
55 World Bank, Privacy by Design: Current Practices in Estonia, India, and Austria, 2018.
56 Database of Aadhar-related forgeries, fraud;.
57 WRIT PETITION (CIVIL) NO. 494 OF 2012.
58 UIDAI, Circular on Enhancing Privacy of Aadhar Holders, January 10, 2018, accessible at: https://uidai.gov.in/images/resource/UIDAI_Circular_11012018.pdf.
59 Information Technology (Intermediaries guidelines) Rules, 2011.

a workable consent framework, while also factoring in various limitations as to scope, purpose and time.

In addition to the above, an effective and accessible consent framework must be mobilised. Such a framework must account for specific requirements of Indian consumers relating to language, literacy levels, etc. Privacy policy documents detailing data management practices should also be made available online in easily consumable formats in a variety of languages.

The flaws in the Aadhaar system in terms of ghost beneficiaries and fraudulent authentication are also required to be plugged if it is to serve as a unique ID for digital transactions. The existence of such a single identifier is crucial to various aspects of an efficient digital ecosystem, such as single sign on feature and pre-filled/personalised forms across various ministries and departments of the Government. In addition, close to a billion people worldwide and a sizable chunk in India, have no legal identity as a result of them being migrants and refugees. Not only should an overarching framework successfully identify citizens, it must also grant some form of digital identity to people without recognised legal status so that basic services may be delivered to them.[60]

The above suggestions along with principles in the Whitepaper help create an environment where users can exercise their rights over their data in a meaningful and effective way. This must be supplemented by appropriate education programmes and information campaigns to enable citizens to exercise their choice in an informed manner and extract the maximum benefit from the creation of open digital ecosystems in terms of service delivery, accountability and transparency.

(c) Exclusion and Digital Divides

The objective of the NODE is to increase the digitisation of services thereby making service delivery more efficient, while offering citizens greater choice and information. Such a system is usually only successful when the foundational infrastructure is in place to ensure that all citizens can access such services and no one is left behind[61]. In ensuring greater participation, the system must be guided by factors of availability, accessibility, affordability, value, and trust[62]. However, Indian society currently suffers from various disparities in access and abilities across the following dimensions/constructs:

(i) Location, Access and Education

Despite recent initiatives such as BharatNet, which has sought to connect every village in the country to a broadband connection, the rural-urban disparity in access and usage of mobile services and the internet remains stark. This is illustrated by the overall tele-density, which stands at 156.26% for urban areas and 56.67% for the rural areas as of 2018[63]. Internet

[60] The World Bank. Global Dataset - Of the 1 billion people without an official proof of identity, accessible at: http://id4d.worldbank.org/global-dataset.

[61] Pathways for Prosperity Commission, The Digital Roadmap: how developing countries can get ahead, Final report, Oxford, UK 2019.

[62] McGowan, Vora, , Homer, and Dolan., Personal data empowerment: restoring power to the people in a digital age, Pathways for Prosperity Commission Background Paper Series; no. 11. Oxford, United Kingdom, 2018, accessible at: https://pathwayscommission.bsg.ox.ac.uk/sites/default/files/2018-11/personal_data_empowerment.pdf.

[63] Telecom Regulatory Authority of India, Highlights of Telecom Subscription Data, December 21, 2019, accessible at: https://main.trai.gov.in/sites/default/files/PR_No.17of2020_0.pdf.

penetration similarly highlights this digital divide[64]. The lack of access is further compounded by digital illiteracy and an acute lack of any training or technological skill development in rural areas.

In comparison, Estonia, one of the countries used as a case study in the Whitepaper, boasts widespread access to 4G (96% of the population) and other forms of high-speed internet. Disparities in digital literacy across rural urban areas are also far smaller than that in India[65].

Given that numerous government schemes and services are targeted specifically at the rural areas, increasing digitisation of services without simultaneously increasing availability of access and improving literacy can result in significant exclusions while exacerbating existing disparities.

(ii) Gender

The deep-rooted gender inequality in India extends to the digital sphere. Men are twice as likely to be Internet users as women in India[66], and a woman is 28% less likely than a man to own a mobile phone[67]. Therefore, a push towards digital ecosystems runs the risk of leaving out a significant number of women, particularly those living in rural areas.

(iii) Age

India has a predominantly young population and is expected to have one of the largest working populations in the world by 2025. Despite being a small number, people above the 60 years of age are particularly vulnerable and rely heavily on government support and service delivery. In this context, it is pertinent to note that less than 5% of those aged 60 and above are able to operate a computer[68]. Furthermore, while people above the age of 45 constitute 18% of the population[69], they comprise only about 6-7% of internet users in the country.

While the divides stated above are significant, particularly in the Indian context, they are by no means exhaustive. Any overarching framework or policy dealing with a NODE must also account for divides that exist across socio-economic strata, including caste. This is of particular significance as access, availability and ability to use are closely related to one's economic profile and standing in society, in addition to factors identified above.

Suggestions for overarching guidelines and or regulatory framework

Principle 11 of the Whitepaper recognises the importance of inclusiveness in the creation of a digital ecosystem. To this end, suggests ensuring the availability of content in all vernacular languages, adoption of user-friendly

[64] 51% for urban areas and 27% for rural areas, per Internet and Mobile Association of India, India Internet 2019, accessible at: https://cms.iamai.in/Content/ResearchPapers/d3654bcc-002f-4fc7-ab39-e1fbeb00005d.pdf.

[65] European Commission, Digital Economy and Society Index 2018: Country Report - Estonia, accessible at: https://ec.europa.eu/information_society/newsroom/image/document/2018-20/ee-desi_2018-country-profile_eng_B43FFF58-F3FD-633C-F5833D8295BB9EB0_52221.pdf.

[66] Internet and Mobile Association of India, India Internet 2019, accessible at: https://cms.iamai.in/Content/ResearchPapers/d3654bcc-002f-4fc7-ab39-e1fbeb00005d.pdf.

[67] GSMA, the Mobile Gender Gap Report 2019, accessible at: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/02/GSMA-The-Mobile-Gender-Gap-Report-2019.pdf.

[68] Council for Social Development, Digital Literacy Training to Non-IT Literate Citizens Impact Assessment of the National Digital Literacy Mission, accessible at: http://www.csdindia.org/pdfs/Project-reports/Digital-Literacy-Report-2017.pdf

[69] http://censusindia.gov.in/Census_And_You/age_structure_and_marital_status.aspx

UI/UX designs, and use of multiple and simple formats, such as text messages and IVRS for the delivery of services.

While these are steps in the right direction, they do not, by themselves, help overcome the multiple digital divides highlighted above. For instance, no solutions are provided for citizens who do not possess a mobile phone or an active telephonic subscription.

That would require a concerted effort to build infrastructure, increase awareness, and promote the large-scale use of digital ecosystems and ICT based technologies. Achieving these objectives is likely to take a significant amount of time and requires collaboration between various stakeholders across the spectrum. Guidelines and regulations dealing with the establishment of the NODE must facilitate such infrastructure development and allow for such collaboration in the longer run.

In the meanwhile, efforts must be made to simplify the means of accessing digital services while also continuing to provide services in their physical form for the next few years, through common service centres or otherwise[70]. Adopting a 'digital first' approach, as espoused in the Economic Survey 2018-19[71], and providing services solely through digital means can possibly exclude a large number of citizens and deny them benefits they are otherwise entitled to. Therefore, it would be appropriate to adopt a bottom up approach to the creation of a NODE which focuses on building capabilities and capacities of all stakeholders while also simplifying methods and procedures to create a truly inclusive ecosystem.

Q14. HOW WOULD YOU LIKE TO ENGAGE FURTHER (E.G. INDIVIDUAL CONSULTATIONS, WORKSHOPS, ETC.) AS WE BUILD THE STRATEGY FOR NODE?

We greatly appreciate that MEITy endeavours to formulate the NODE governance framework in a consultative manner and account for the views of multiple stakeholders. We would be happy to engage further in developing this framework through written submissions on targeted issues, workshops, consultations, and other methods of engagement that MEITy may formulate.

[70] https://www.apc.org/sites/default/files/APCProPoorKit_CaseStudy_SomeLessonsFrom%20India_EN.pdf

[71] Economic Survey, 2018-19, Chapter 4: Data of the People, By the People, For the People, accessible at: https://www.indiabudget.gov.in/budget2019-20/economicsurvey/doc/vol1chapter/echap04_vol1.pdf

*This document has been prepared by the Fellows at the Esya Centre.
For any further contact, please get in touch with us at:*

www.esyacentre.org

ESYA
centre