Response to the White Paper on the Strategy for National Open Digital Ecosystems released by the Ministry of Electronics and Information Technology in February 2020

Dvara Research[1] is an independent Indian not-for-profit research institution guided by our mission of ensuring that every individual and every enterprise has complete access to financial services. Our work seeks to address challenges for policy and regulation in India including in the waves of digital innovation sweeping financial services, focussing on the impact on lower income individuals in the country. The regulation of personal data and public digital infrastructure have been core areas of our recent research.

In this document, we present our response to the White Paper on the Strategy for National Open Digital Ecosystems (the White Paper) released by the Ministry of Electronics and Information Technology (MeitY) in February 2020. We are deeply concerned that creating National Open Digital Ecosystems (NODEs) as envisioned in the White Paper could entrench existing problems with service delivery and hamper the growth of a free and fair digital economy. The assumptions, principles and strategies underlying NODEs merit re-consideration. To begin a constructive conversations on these issues, we present research and responses to public consultation in this document in two sections.

Section I of this response presents five overarching concerns with the White Paper (set out below), with detailed analyses and recommendations to address these concerns.

1. The need and objectives driving the creation of NODEs are unclear, as are the basis for the fifteen Guiding Principles guiding the design of NODEs delivery platforms.
2. Purpose-agnostic NODEs without clear legislative backing would defy constitutional requirements that public digital systems must have specific and legitimate purposes to exist.
3. The operational model for NODEs in the White Paper can create challenges for Transparency, Governance and Accountability.
4. Digital-by-default governance strategies and poorly designed public digital infrastructures can create risks of exclusion and distress for low-income, marginalised communities. Any strategy for NODEs must learn from India's past experience.
5. NODEs can pose severe risks to competition and systemic stability.

Section II presents our specific responses to the "*Key Questions for Consultation*" presented in Chapter 7 of the White Paper.

We welcome any opportunity to present this research or respond to questions and comments on our research to MeitY.[2]

[1] Dvara Research has made several contributions to the Indian financial system and participated in engagements with many key regulators and the Government of India. Through our recent work we have extended research inputs to bodies including the Committee of Experts on Data Protection under the Chairmanship of Justice B.N. Srikrishna, the Ministry of Electronics & Information Technology (MeitY) and the RBI's Committee on Deepening of Digital Payments. Our primary research on Indians' privacy & data sharing attitudes was cited in the 2017 White Paper of the Expert Committee on Data Protection under the Chairmanship of Justice B.N. Srikrishna. Our regulatory proposals on enforcement and the design of the Data Protection Authority (DPA) were specifically acknowledged and relied upon in the Final Report of the Committee dated 27 July 2018.

[2] The corresponding author for this publication can be contacted at srikara.prasad@dvara.com.

TABLE OF CONTENTS

I. Overarching comments on the White Paper

1. The need and objectives driving the creation of NODEs are unclear, as are the basis for the fifteen Guiding Principles guiding the design of NODEs delivery platforms.

The White Paper (at page 34) describes NODEs as a paradigm shift from the current "*GovTech 2*.0" to an ecosystem-based approach that can "*transform service delivery and create shared value for all stakeholders in the ecosystem*".

While the ambitious vision of the White Paper is appreciated, the objectives and need for NODEs in India are not clearly articulated in the White Paper. Other digital infrastructure projects in India (such as the RBI's Public Credit Registry) and globally (such as the UK's National Digital Twins) begin with a clear articulation of the motivations and need for the architecture, justifying the impact on citizens and the spend from the exchequer.

The absence of these objectives also creates ambiguity regarding the fifteen Guiding Principles (at Chapter 4 of the White Paper) that will guide the design and build of the NODEs. There are no clear objectives against which to assess these principles, and consequently whether they serve to fulfil the right motivations and objectives.

We flesh out both these concerns below i.e. (i) that clear objectives must guide public policy choices of this magnitude, (ii) the basis for the Guiding Principles need to be clearly articulated, and tied back to objectives.

1.1. Precise objectives and motivations for NODEs and how they will improve service and welfare delivery must be set out in the White Paper

Clear identification of problems and clear articulation of objectives are central to policy formulation as they provide a basis for identifying policy priorities, design and objectives (Sabatier & Mazmanian, 1980) (Jordan & Turnpenny, 2015). It is well-recognised that a lack of clarity on motivations can adversely affect the design, implementation and effectiveness of a policy (Van Meter & Van Horn, 1975).

A failure to achieve clarity on motivations could have severe adverse implications for the future design or implementation of NODEs. The White Paper does not articulate precisely the problems that it is trying to address and articulate with adequate detail the objectives that it seeks to achieve. Instead it broadly refers to potential gains without setting out how these will be achieved through NODEs, as seen in the following language:

> "*Such shared digital infrastructure has the potential to make governance truly citizen-centric, by simplifying and easing citizens' interactions with the government. At the same time, this can also spur innovation driven by entrepreneurs who build solutions on top of such 'digital rails'...*

[B]uilding an enabling ecosystem to leverage digital platforms for transformative social, economic and governance impact, through a citizen-centric approach." (page 4 of the White Paper).

Examples of clearer articulations for large information infrastructures already exist, for instance in the Report of the High-Level Task Force on the Public Credit Registry (PCR) discussed in Box 1 below (High-level Task Force on Public Credit Registry, 2018).

Box 1: The Report of the High-Level Task Force on the Public Credit Registry (PCR)

The PCR is a credit information repository that was envisioned by the Reserve Bank of India to address problems that were affecting the quality of credit information in the Indian financial sector. The Report of the High-Level Task Force on the PCR (the Report) provides an example of another recent policy document seeking to create a new digital infrastructure in India.

Identifying challenges to be addressed: The PCR Report identifies and articulates problems that the new digital infrastructure seeks to address (at page v):

> "*At present, credit information is spread over multiple systems in bits and pieces. Information on borrowings … are not available in a single repository. This makes it very difficult to form a comprehensive view of total indebtedness of a borrower. Also, essentially the same information gets reported to multiple agencies in different formats leading to inefficiency in the credit reporting system and data quality issues while increasing the reporting burden on credit institutions.*"

In addition, six clear problems with the existing credit information system in India are identified that the PCR Report seeks to address (pages 23 to 25 of the PCR Report): (i) lack of comprehensive credit data (ii) fragmented information that is stored in different formats across different databases (iii) dependency on self-disclosure by borrowers which does not always provide a holistic view about their paying capacity (iv) lack of mechanisms to validate existing information (v) time lag in updating credit information and (vi) multiple reporting of credit information. Irrespective of the assessment of these issues, the PCR Report clearly identifies them.

Articulating objectives: The report finally provides specific objectives that the PCR seeks to fulfil, for instance (at page 43 of the PCR Report):

> "*With the objective of making credit available to those without a recorded credit history and to enable flow based lending, the PCR would collect/facilitate linkage to ancillary credit information, such as utility/statutory/insurance payments data, GSTN data etc subject to the extant legal provisions.*"

While these objectives could be even further fleshed out, this is one example of the kind of articulation seen in a recent Indian policy document.

The White Paper does not clearly set out the motivations driving the idea for NODEs or how NODEs will directly solve or address particular identified issues. The absence of clear motivations for transitioning to NODEs can adversely affect its objectives, its guiding principles, technical and institutional design, which could be expensive for Government as well as potentially create adverse outcomes for users and the system as a whole for reasons set out in the sections I.4 and II.7 in this document.

1.2. The basis for the Guiding Principles needs to be clearly articulated, and tied back to objectives

The White Paper identifies fifteen Guiding Principles in Chapter 4 for designing delivery platforms to create "*transparent governance*" and build a "*vibrant community*" on NODEs. These principles are expected to help NODEs in maximising economic, social and governance benefits for India in a responsible manner (Ministry of Electronics and Information Technology, 2020).

This raises concerns for two reasons.

First, the basis for these fifteen principles is not clear. The principles appear to be suspended in a vacuum without being rooted in the objectives and purposes of NODEs. In the current form, there is a risk that the principles will be interpreted and moulded in ways that suit self-interests of different participants in the absence of a clear foundational basis. This can threaten the safety and effectiveness of NODEs.

Second, there is a lack of symmetricity within the White Paper: while the objectives and reasons for creating NODEs are unclear, there is great detail on Guiding Principles for design. This creates a contradiction or potential for ambiguity, since it is not clear which objectives the design principles are supposed to be fulfilling or maximising.

A good example of how clear objectives can be set up-front, and lead the choice of design principles is found in the UK's Gemini Principles (see Box 2) (Centre for Digital Built Britain, 2018). Interestingly, these are cited in the White Paper.

The White Paper should have clearly articulated the core objectives that justify the reasons for NODEs to exist. Further, it should articulate the relationship between objectives and the Guiding Principles identified.

Box 2: The Gemini Principles

The Gemini Principles guide the development and framework of the National Digital Twins (NDT) in the United Kingdom which perform functions that are similar to NODEs. The Gemini Principles seek to "*help the industry develop digital twins in an aligned way that can become part of the NDT*" (Centre for Digital Built Britain, 2018). These principles are anchored to three underlying objectives (i) Purpose (ii) Trust and (iii) Function, which represent the fundamental ideology of the NDT which cannot be breached.

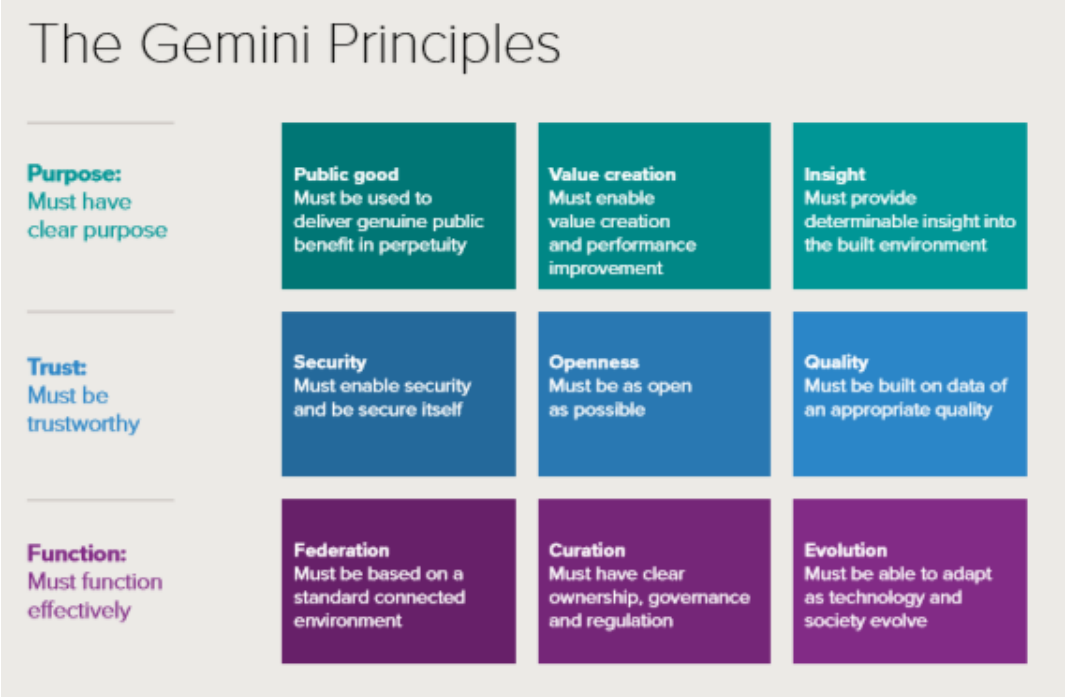

Figure 1: Gemini Principles. Source: Page 7, The Gemini Principles (Centre for Digital Built Britain, 2018).

For example, the second underlying objective, "*Trust*", requires entities to be trustworthy and be ethical by design so that participants feel confident to contribute to the NDT. It further requires governance and regulatory frameworks within NDT to be transparent, open and effective to uphold trust. Three principles anchor around this core objective (Centre for Digital Built Britain, 2018):

i. Security, which requires the NDT to be secure and enable security to uphold trust.
ii. Openness, which requires the NDT to be as open as possible without impinging on security.
iii. Quality, which requires NDT to be built on data that is of good quality.

This framework demonstrates the clarity that can be achieved with respect to objectives to which clear and simple principles can be anchored.

2. Purpose-agnostic NODEs without clear legislative backing would defy constitutional requirements that public digital systems must have specific and legitimate purposes to exist.

The White Paper appears to enable the creation of an indefinite number of NODEs through the creation of multiple delivery platforms that are interoperable across government departments. In effect, this would connect different data registries, data exchanges and stacks. This enables the sharing and exchanging the personal information of all Indian citizens, ostensibly in order to (i) eliminate multiple touchpoints between government and the citizen, (ii) allow different government departments to collaborate for service delivery and (iii) allow private players to build new services and solutions on top (page 4 of the White Paper).

When creating such a largescale information infrastructure that will pool, share or interconnect the personal data of millions of citizens, there is an obligation to act lawfully, legitimately and proportionately to benefit rather than harm the interests of citizens. India has evolved a legal test to be applied for every infrastructure which seeks to aggregate personal data in this manner to ensure that it does not infringe the informational privacy of a citizen—and in cases where such infringement is likely to occur, that it must be lawful, legitimate and proportional within a system of accountability. The creation of multiple NODEs and the usage of personal data on NODEs should:

- not be contemplated without clear legislative framework which bears in mind constitutional requirements. The White Paper does not indicate the creation of any such laws for NODEs; and
- not be contemplated without identifying a specified, limited, pre-determined purpose, as required by well-recognised data protection principles.

The White Paper mentions (on page 8) that the NODEs will have a governance framework of which one element will be data privacy (including laws & regulations to protect personal and non-personal data). However, there is a need for a full legislative framework for a NODE folding in various aspects of governance including data protection and privacy.

NODEs should not be contemplated without a clear legislative framework.

The need for a legislation to support the creation of large-scale digital databases is both a constitutional requirement and a significant learning from India's experience of creating the Aadhaar database and IndiaStack.

The Unique Identification Authority of India (UIDAI) was first created in 2009 as an office of the Planning Commission. The need for a legislation to collect citizens' personal data on a large scale and to extend parliamentary scrutiny to the UIDAI was realised as early as 2010, but the Aadhaar Act itself was only passed much later in 2016 (Pathways for Prosperity Commission, 2019). This created legal

and operational uncertainty for the entire ecosystem, especially as the question of the legality of the entire project was ultimately placed before the Supreme Court. Along with uncertainty, this has also raised issues of mistrust and rushed implementation that any future attempts to build digital infrastructure must pay heed to.

A lack of parliamentary backing and scrutiny would set back the legitimacy of NODEs, and also have serious implications for rights of citizens and safety / opacity of the country's digital infrastructure.

Therefore, the creation of NODEs needs to be supported by a legislation. Such legislation needs to be in line with the three part-test set out in *Puttaswamy v Union of India* (2017) (the Privacy judgment). This test requires state actions relating to users' personal data need to be–

i. sanctioned by a law,
ii. necessary for pursuing a legitimate state aim, and
iii. proportionate to this aim i.e. there cannot be unbridled access to personal data and it should be the least intrusive measure connected to the purpose of fulfilling this aim. (*Justice K.S. Puttaswamy (Retd) & Anr v. Union of India & Ors, 2017*).

As NODEs seek to connect databases of citizens' personal information, they will have to satisfy this test to be constitutionally valid. First, the creation of NODEs will have to be backed by a suitable legislation. Second, that legislation must justify that the creation of bigger databases containing potentially richer, more sensitive personal information than that found in isolated datasets is necessary for pursuing a legitimate state aim. It will have to be proven on merits that NODEs are necessary for pursuing a legitimate state aim. Third, the legislation will also have to demonstrate that the creation of NODEs is proportionate to the specified purpose and least intrusive.

Further, future legislation that could allow the creation of NODEs cannot legitimise the blanket interlinkage of subsequent databases. Each interlinkage of databases needs to fulfil necessity and proportionality. This requirement is clearly given in the Supreme Court's judgment in *Justice K.S. Puttaswamy v Union of India* (2018) (the Aadhaar judgment). The Supreme Court struck down the compulsory linking of the Aadhaar with new and existing bank accounts to prevent money laundering and determined it to be *grossly disproportionate* vis-à-vis the purpose cited (Misra, Sikri, & Khanwilkar, 2018) (Chugh & Raghavan, 2019). The judgement further recommended the state to address its concern of suspicious transactions by undertaking a better targeted study of such persons and their means, instead of mass surveillance (Chugh & Raghavan, 2019). Every interlinkage between a database therefore needs to be tested against the test set out in the Supreme Court's Privacy judgment to ensure they are indeed **proportionate to a specific purpose** that is identified in advance.

Accordingly, NODEs must be created for a clear and legitimate purpose through a law passed by Parliament which proves the necessity and proportionality of such a system.

3. The operational model for NODEs in the White Paper can create challenges for Transparency, Governance and Accountability.

NODEs are envisioned to perform public functions of welfare delivery, and other services. They will be using large swathes of the personal information of the Indian public, and their financing model may involve support from the State (in terms of funds from the exchequer, subsidies or other enabling public finance strategies).

In these circumstances, the governance of NODEs must be held up to the level of accountability required from all public institutions in terms of audit, oversight and transparency.

3.1. Misaligned incentives between government and co-opted private entities can lead to unfavourable outcomes.

The White Paper emphasises on active participation from private entities for building, financing and looking after the administration of NODEs (Principles 6, 9, 10 & 14). Care should be taken to ensure that the incentives driving public entities and private entities on NODEs are aligned with each other. The involvement of private players in service delivery conflates citizens and consumers. It is important to identify the distinction between users as citizens who are *entitled* to services and users as consumers who can *opt for* or *purchase* services.

A multi-stakeholder approach like that suggested in the White Paper requires adequate incentives to encourage participation from both private and public sector players. Inadequacy of financial and non-financial incentives can discourage private entities from engaging with NODEs, or alternatively encourage them to create perverse incentives such as charging end-users excessively (Gupta, 2020) (Anognya & Gupta, 2020). Different incentive structures will have to be developed based on the nature of the NODEs being discussed to avoid incentive misalignments.

For instance, in the context of the State Service Delivery NODE (SSDN) (described in Chapter 5 of the White Paper), alignment of incentives becomes crucial both at the back-end as well as at the front-end. Governments must incentivise adequately to encourage participation from Technology Service Providers (TSPs) for seamless functionality of NODEs. The efficient functioning of the core technology is the base upon which digital ecosystems are built. Co-opting the right technology partner that can create the right technology base for digital infrastructures therefore becomes critical. The wrong model can also set back critical service delivery.

Past experiences in India and other countries provide cautionary tales of instances where technology infrastructures suffered serious setbacks when private players were co-opted into delivery. They created high costs for the government or poor performance on outcomes due to misalignment of incentives and failure of safeguards.

i. *The digital platform for Obamacare*: The digital manifestation of the US Affordable Care Act titled *healthcare.gov* was a platform meant to serve as a government-run marketplace for medical insurance (Baker, 2014). However, uncertainty over the requirements of the marketplace coupled with bad contracting practices of the government led to the creation of a platform that was plagued by technical problems and software glitches. Users were unable to sign up for health plans until the platform was fixed many months after it suffered setbacks at launch (Pickert, 2014). The government ended up spending USD 840 million on the platform including more than USD 150 million just in cost overruns for the version that failed. Other projects including portals for administration and job searches in the USA show similar problems with co-opting private entities for building large-scale digital infrastructures that lead to delay, high overhead costs and inability to meet user expectations (Tanfani, 2013) (Lipowicz, 2011).

ii. *The Queensland Health payroll system*: The Australian government sought to create a "whole-of-government human resources and finance solution" that, among other things, provide payroll and rostering system for public servants (Moore, 2013). However, it appears that similar shortcomings in the contracting process and lack of certainty about performance criteria led to similar outcomes as *healthcare.gov* in the USA. The platform failed entirely resulting in thousands of health workers being underpaid, overpaid or not paid at all; and cost the Australian exchequer 1.2 billion dollars (The Sydney Morning Herald, 2016).

iii. *India's Central Know Your Customer Registry (C-KYC)*: The C-KYC is meant to compile all KYC data of users across financial sectors. The main objective of the C-KYC is to eliminate the need for users to repeat their KYC process each time they interact with a new financial service provider. This required different financial regulators such as the banking regulator, securities regulator and others to share their KYC data for the creation of C-KYC. However, lack of standardised data, lack of APIs to share the data and inconsistent distribution of costs setback the creation and implementation of the C-KYC. This slowed the implementation process, increased the costs of the project and inconvenienced the consumers, who bear the costs of unwieldy (and uncertain) KYC processes (Chugh & Raghavan, 2019), (Business Line, 2018).

This suggests that creating common data repositories can be ineffective without focusing on deeper issues such as technical compatibility between a variety of institutions, quality of data that is reported incentives for participants (Chugh & Raghavan, 2019). Further, lack of clarity in contracting can compromise the functionality of the infrastructure and limit its ability to serve the intended objective.

Government must therefore ensure that the monetary and other incentives of the participants are well-aligned. This would need to be buttressed by a strong system of accountability and governance, to ensure private participants best serve the consumer and reduce the scope of perverse practices such as

unforeseen rent-seeking as uncovered for instance by research on common service centres (CSCs). CSCs created under the Digital India Mission (2015) to facilitate access to digital services at the last mile sometimes charging consumers for "free services" such as facilitating banking transactions, or overcharging other service fees stipulated by the Government (Anognya & Gupta, 2020).

Further, it is essential to align stakeholders on the standards of technology, processes and protocols, and ensure that the upcoming infrastructure serves the requirements of each stakeholder. Any lapse could compromise the functionality of the infrastructure, increasing costs and adversely affecting users' experience.

3.2. Private entities involved in NODEs must be held up to scrutiny and accountability standards of public authorities undertaking public functions. All entities involved with NODEs must have strong complaints handling and grievance redress systems.

Principle 6 (on page 17 of the White Pape) requires NODEs to have a single point of accountability and to identify:

> "*an accountable institution for each delivery platform, whether a public or a private body or a coalition set up as a Special Purpose Vehicle (SPV) or Public Private Partnership (PPP), which is responsible for the overall administration of the platform and setting the standards or rules of engagement that drive accountability. Finally, organization structures, platform resourcing and performance management all need to align with these frameworks.*"

This Principle is a serious concern, and must be replaced by the requirement for publicly accountable institutions to drive NODEs.

Entities involved in NODEs must be publicly accountable to the standards of all public authorities undertaking public functions

Principle 6 appears to be opening up the option for institutions that are not accountable to the public to be handling and accessing troves of citizens' information from Government and undertaking public service delivery without being subject to the accountability requirements of public sector institutions such as audits, compliance with the Right to Information Act, etc. Giving private entities that are not accountable to the public control over a delivery platform raises two kinds of concerns (i) enforcing accountability against the entity becomes difficult and (ii) it creates a risk of moral hazard where the entity can violate the principles of institutional neutrality.

There is limited scope to enforce fundamental rights of citizens against private players, even when they perform essential state functions (Kumar, 2020). Private players would also be outside the scope of other formal grievance redressal mechanisms such as the Right to Information Act, 2005. Together, these could result in diminished accountability of the private player and citizens having little recourse against the private players if there are any grievances arising from their services.

Principle 6 in the White Paper offers the policy-choice of building NODEs with an expanded role for private entities including private entities controlling the overall administration for certain NODEs. Further, institutional neutrality in regulation is indispensable for creating a level ground and promoting competition in the market. Letting some private entities exert disproportionately high influence over the administration and standard setting over NODEs, we run the risk of encouraging moral hazard and dampening competition among players. Private entities on NODEs, may be inclined to impinge on the principles of neutrality by creating self-serving rules of engagement or by entrenching their own technology and software as standards for the delivery platform. For instance, such an arrangement, where the government completely divests its control over the infrastructure could also have the effect of entrenching proprietary software. This raises issues of vendor lock-in, lack of accountability and incentive misalignment that may limit the government's ability to modify the software or to use it for any other purpose.

Principle 6 could set back the transparency and accountability of NODEs in its current form, and must be re-considered to ensure better incentive alignment and accountability of NODEs to the public. Not doing so, could lead to unaccountable entities gaining control over licensing of technology and software that process all citizens' data, potentially violating the principle of openness (Principle 1) also aspired to by NODEs.

All entities involved with NODEs must have strong complaints handling and grievance redress systems

NODEs envisages an ecosystem that will contain several public and private entities performing a variety of functions and operations. It would be very difficult for users to grasp the nuances of NODEs, identify points of liability, identify the relevant sectoral regulator and engage with multiple entities for seeking redress for various kinds of risks and harms they will face. While customer support helplines are one of the grievance redressal mechanisms in NODEs, these are merely a starting point. There is a need to set up a complete grievance redressal system at the heart of the NODEs infrastructure, given that their main activity seems to be sharing of the personal information of millions of individuals and delivery of services to them. Any grievances in this process need to be immediately managed to avoid distress and harm to individuals.

One relevant blueprint for a unified redress agency in the financial sector exists in the Report of the Financial Sector Legislative Reforms Commission (FSLRC) (Financial Sector Legislative Reforms Commission, 2013). This is pertinent to NODEs, given the need for simple and effective grievance redressal across sectors. The Financial Redress Agency (FRA) was proposed in the FSLRC to simplify redress in the financial sector which has "*multiple laws and regulated by multiple agencies covering various sectors*" (Financial Sector Legislative Reforms Commission, 2013). The FRA was envisaged to provide a consumer-facing front-end at the district level where complaints regarding all financial

products can be registered. Following registration, the FRA would channel the complaint to the appropriate regulator, and entity in the backend through technology-intensive processes for resolution via mediation and light-weight adjudication (Task Force on Financial Redress Agency, 2016).

Such a sector-neutral grievance redressal structure would considerably reduce the burden on users to identify the points of liability, identify the regulator or entity and then lodge a complaint. Additionally, the FRA was envisaged to serve as an efficient feedback mechanism which can identify points of weakness in the financial system based on the complaints received and inform better regulation making (Financial Sector Legislative Reforms Commission, 2013).

Adopting such a grievance redressal mechanism in each NODEs is crucial for effective user protection. International best practices also suggest that local and multiple grievance redressal access points are essential for an effective grievance redress system. Such a system in turn instils confidence in users and encourages them to approach the system for redress more frequently (Dvara Research, 2018).

NODEs must provide unified grievance redressal front-end at the local level like the FRA with effective back-end adjudication processes to provide users easy access to effective grievance redress. Further, adopting such a grievance redressal mechanism will be beneficial for NODEs in fulfilling its own objectives of:

i. *Single touchpoint for users*: NODEs seeks to provide a single touch-point for users for interacting with public and private provider entities. Creating a single touch point for grievance redressal would further this objective.
ii. *Strong feedback loops*: NODEs will have to (a) understand the challenges that are impeding operations (b) identify and mitigate risks of harm to the user and (c) identify gaps in regulation so that they can gain traction and mobilise a wider community of participants. A unified front-end for grievance redressal like the FRA for NODEs will be able to serve as an effective feedback loop that can analyse user complaints and highlight weakness in the ecosystems. Further, the unified front-end agency can be required to publish periodical reports of grievances raised and actions taken to ensure transparency.

Customer helpline numbers can be one of the means through which users can access the unified grievance redressal front-end of a NODEs. In addition, users should be allowed to ask for redress via written letters or e-mail, fax, telephone, missed call services, online portals, mobile apps, SMS and video to significantly improve access to this grievance redressal front-end (Task Force on Financial Redress Agency, 2016). The grievance redressal mechanism should also provide users visibility into the grievance redressal process by allowing online as well as offline tracking of their complaints for transparency (Dvara Research, 2018).

Accessible and effective grievance redressal frameworks are crucial for strong user protection in NODEs. Grievance redressal mechanisms must be *fast, transparent and easy to understand* to be effective. They must not burden users by requiring them to be well versed with statutory provisions so that grievance redressal is accessible to all users without being limited by literacy and quality of education (Dvara Research, 2018).

3.3. For NODEs to be transparent and accountable, and "open" as public digital infrastructure they must not be built with proprietary software.

The White Paper envisions NODEs to be an open digital ecosystem that is anchored by transparent government mechanisms. While the degree to which NODEs would be "open" will depend on the sector and purpose for which they are created, care must be taken to ensure that proprietary interest over the software does not override the interests of openness in public welfare delivery.

The principle of openness represents a set of values that include transparency, access, participation, and democracy (Schlagwein, Conboy, Feller, Leimeister, & Morgan, 2017). Openness is therefore a tool for ensuring visibility and accountability for the functioning of a code. Openness should not be subdued in the interests of proprietorship especially in case of public welfare delivery.

The use of proprietary software for fulfilling public purposes may cause some concerns about accountability and the right to use software. Proprietary software does not allow auditability and can lead to vendor lock-in issues that have a grave impact on public service delivery as witnessed with many public service delivery programs globally (World Bank Group, 2019).

Using open source software to operate public service delivery NODEs is one step towards greater transparency and better accountability in NODEs. The term "Open Source" generally involves enabling inspection of the software's source code, and also often enables (i) free redistribution of the source code at a reasonable cost (ii) license to modify the source code (iii) license to distribute the program built through modifying the source code (iv) access for all persons irrespective of the field of endeavour and (v) automatically transferrable rights over using the source code and the modified program (Open Source Initiative, 2007).

Open source software creates two benefits for stakeholders. First, they can engage a wider community of stakeholders without facing the limitations created by proprietary software. This allows stakeholders to collaborate to innovate and create better solutions on top of the existing code. Stakeholders will be able to create highly tailored and diverse set of solutions for service delivery.

Second, open source codes allow greater visibility into the functioning of the code, promoting auditability, accountability and quality. This can help public authorities to identify and address problems with a code expeditiously (AlMarzouq, Zheng, Rong, & Grover, 2005). Reference can be made to Estonia's Public Codes Registry which is based on open source technologies that allow

complete visibility into the code. That Registry allows anybody to access and use the open source code unless there are compelling security reasons to not allow access (E-Estonia, 2019). Using open source codes helped the Estonian authorities to rectify cyber vulnerabilities expeditiously at little cost (E-Estonia, 2018).

4. **Digital-by-default governance strategies and poorly designed public digital infrastructures can create risks of exclusion and distress for low-income, marginalised communities. Any strategy for NODEs must learn from India's past experience.**

The White Paper (at page 1) lays the foundation for building an enabling ecosystem called NODEs in India that will "*leverage digital platforms for transformative social, economic and governance impact*…". Countries across the globe are at various stages of creating digital infrastructure and governance structures for them.[3]

The design of a future digital infrastructure should be informed by our own Indian experience of digitisation and technology-adoption to date, as well as relevant global experience. Any proposal for NODEs or other Indian digital infrastructure must take into consideration the realities below to prevent exclusion.

4.1. A push for digital-by-default policies can lead to a system of exclusion-by-design.

The digital-by-default approach taken by NODEs is a marked shift from the other past approaches that provided offline touchpoints for users. The digital-by-default approach works on the premise that all users are online, digitally skilled and confident to make claims through an online portal. Therefore, face-to-face, telephonic and paper-based interactions can be replaced by web-based services, mobile apps or other digital touchpoints.

Such an approach can have adverse implications for service delivery, especially for public service delivery directed at poorer and more vulnerable users. This has been recognised even in advanced economies where the majority of the population has access to high speed internet, mobile and computing devices.

For instance, the United Kingdom's Universal Credit program (UC program) which followed a digital-by-default approach to service delivery suffered the consequences of this approach. The UC Program was the first service delivery program to become digital-by-default in the UK in 2013. It required users to make claims for social security benefit payments from government online and to interact with authorities through an online portal (Government Digital Service, 2017). The completely digital format

[3] *See* 'Emerging Data Sharing Models to Promote Financial Service Innovation: Global trends and their implications for emerging markets' *by Rafe Mazer for learnings about design and governance of different kinds of open digital ecosystems in countries like Kenya and China that are similarly placed to India (available at s3-eu-central-1.amazonaws.com/fsd-circle/wp-content/uploads/2018/07/12111727/Emerging-Data-Sharing-Models-to-Promote-Financial-Service-Innovation-June-2018-Mazer.pdf).*

of the program was ill-suited to the most vulnerable households in the UK that were effectively offline. A report submitted to the UNHCR in 2018 found that only 54% of all claimants can apply online without assistance (Special Rapporteur on extreme poverty and human rights, 2019). The UC program therefore raised significant digital barriers to accessing essential services by excluding those who were most in need of credit support. It had a disproportionately adverse effect on women, older people, persons with disabilities and linguistic minorities (Citizens Advice Flintshire, 2018). Although the UC program allowed claimants to make claims through designated helplines, assessments suggest that the helplines were ineffective to access services.

Further, the UC program used a variety of data points like income to automatically calculate monthly benefits due to claimants. However, errors in these data points and delayed reporting of data points caused major discrepancies in calculating the amounts due to beneficiaries (Special Rapporteur on extreme poverty and human rights, 2019). It is pertinent to note that digital barriers to accessing the UC program were high despite the UK having a literacy rate of 99%.

This reveals that a 'digital-by-default' system could have exclusion built into its very design, since the aged, disabled and marginalised are at the risk of being excluded from essential services. This leaves a gap which needs to be addressed by legitimate intermediators who support access to the system or middlemen. In the case of UK, the public turned to local action groups and public libraries to help them access the digital portal, entities that require further funding from local governments (Special Rapporteur on extreme poverty and human rights, 2019).

In the Indian scenario, a digital-by-default system that is envisaged in the White Paper may be disastrous for millions of low-income and marginalised people who are in high need for benefit delivery. More than a quarter of the Indian population (approximated at 313 million) remains illiterate, of whom 54% are women (Chadha, 2019). A digital-by-default system can increase costs for these and other vulnerable segments of the population who could become victims to rent-seeking behavior from middlemen to profit from the situation. This is currently evident from the practices of the Common Service Centers (CSCs) created under the Digital India Mission (2015) to facilitate access to digital services at the last mile. Our analysis suggests that CSCs often resort to overcharging consumers for stipulated service due to poor economic returns from the business model. A digital-by-default model envisioned for NODEs may be a disservice to millions who do not have access to digital interfaces by entrenching their dependence on middlemen (Anognya, 2020) (Anognya & Gupta, 2020) (Gupta, 2020).

4.2. Opacity, poor accessibility and poor data quality can impose high costs on more vulnerable users.

The White Paper anticipates that NODEs will be able to provide users with a single touchpoint to access a variety of government services. However, single digital touchpoints may not always lead to favourable outcomes for consumers and in some cases are known to increase opacity, reduce accessibility and

reinforce social power hierarchies. Experiences in India, as in the case of the *Bhoomi* project in Karnataka, give some cause for concern.

The *Bhoomi* project was meant to digitise Karnataka's land records in an endeavor to provide proof of land ownership to farmers and landowners in rural districts of Karnataka. While the project was initially lauded for its perceived impact and endorsed as the model project for digitising land records in India, later ethnographic studies suggest that the project resulted in increased corruption (Benjamin, Bhuvaneswari, Rajan, & Manjunatha, 2007). The project increased potential for corruption at various levels by centralising land management by and opening land records to the public (Wright, Abraham, & Shah). Any correction of incorrectly entered land ownership details required several visits to the Taluka offices, which the farmers could not afford in terms of time. This enabled the return of middlemen in the process, creating opportunities for bribes.

Separately, it also created a situation whereby poorer farmers were unable to access the benefits of the project by themselves, but more powerful farmers could take advantage of the system. Computerisation of records allowed larger farmers to use the survey numbers of small farmers to access government schemes and benefits. Larger farmers, in this case, were also found to draw on their links to the judicial and administrative elite to utilise the centrally available data in their favour (Benjamin, Bhuvaneswari, Rajan, & Manjunatha, 2007). Recent examples from Telangana's land digitisation shows similar issues of increased opacity in land management, mismatched land records and lack of proper grievance redressal mechanisms (Mithun, 2019).

Digitisation is often believed to lead to increased transparency and reduce corruption. In practice, India has experienced that digital systems built with opaque back-ends and difficult citizen interfaces can impose high costs on individuals. These experiences suggest that digitisation without considering local power structures and political economy among other factors can heighten vulnerability and create room for corruption. This could be a serious challenge, and the failure to address this (or even indicate awareness of these real-life concerns) in the present design of the NODEs ecosystem and the White Paper could create serious risks in the future.

4.3. Interconnected databases can lead to technology failures at scale.

The White Paper advocates for interconnected databases with the aim of maximizing efficiency across governmental departments. However, data is often collected by various government departments for particular use cases. Interlinking databases without accounting for these purposes and specific features of each database is likely to cause errors at scale and result in high costs for both the citizens and the government (Kodali, 2018).

The notorious *Robo-debt* of Australia is a key case in point. The Australian Department of Human Services initiated a program called *CentreLink* which could automatically detect overpayment of social

security benefits to beneficiaries. To do this, *CentreLink* cross-verified income data reported on its portal with data from other government services databases like the Australian Tax Office. If the program determined that excess dues were paid, it issued a notice to repay the dues as debt (Victoria Legal Aid, 2019).

However, discrepancies caused by relying on data obtained from the Australian Tax Office created large sums of wrongful debts that were charged to beneficiaries (Karp, 2019). The incorrect adoption of cross-departmental data for calculating social security dues imposed significant costs to both the beneficiaries and the government. The government had to incur costs to repay hundreds of millions of dollars that were wrongly collected from beneficiaries, and eventually, overhaul the CentreLink scheme (Henriques-Gomes, 2020).

India has suffered dysfunction for cross-Government interlinking of databases as seen as witnessed while onboarding departments to the National e-Governance Service Delivery Gateway (NSDG) (The Hindu, 2017). In that instance, different State Government departments' inability to adhere to standardised protocols led to poor take-up of the NSDG, and ultimately some States created their own platforms resulting in redundancies and overlaps.

Further, in India, various government departments collect data for distinct purposes. They also collect different information under the same headings (Wright, Abraham, & Shah). Further, the quality of data collected by government departments is not without error as evidenced by the studies on Aadhaar (Khera, 2019). Interlinking different databases via NODEs without being conscious of these challenges risks recreating crises like the Robo-debt crisis, in India.

4.4. Lapses in cybersecurity can render users more vulnerable to economic harms

All digital ecosystems are vulnerable to cybersecurity risks. Estonia's e-government project, *e-Estonia*, provides users access to services exclusively through a chip-equipped card called *eID* that is procured from a single vendor. This eID helps users in authenticating their identity and digitally signing documents for accessing close to five thousand public and private services. However, in 2018 a flaw in the eID card exposed eight lakh eID cards in Estonia and at least 1 billion cards around the world to severe privacy risks by breaking their encryption and allowing access to highly sensitive information (E-Estonia, 2018) (Information System Authority, 2018). Estonia was able to mitigate the adverse effects of this flaw by temporarily suspending the affected cards and allowing users to remotely update their cards. However, other countries including Spain, Brazil, Italy and Austria that used similar cards had to revoke millions of cards at high cost and disruption in accessing essential services (Information System Authority, 2018).

In India, this can have grave implications for peoples' right to privacy and increase their vulnerability to harms caused by a misuse of their personal data. These concerns are further reinforced by earlier

lapses in handling people's personal data as evidenced by many reported breaches of the Aadhaar system over the years (Vidyut, 2018) (Kodali, 2017).

4.5. Authentication mechanisms in addition to Aadhaar must be considered, if NODEs are intended to be created.

The White Paper has expressed intentions to use Aadhaar for uniquely identifying users in NODEs. NODEs must not rely solely on Aadhaar for identifying data records. Other systems (both existing and new) for identification must be considered especially for public service delivery, to avoid exclusion.

First, linking of the Aadhaar database with NODEs can be disproportionate to the purpose of Aadhaar, and therefore violate users' fundamental right to privacy (Justice K.S. Puttaswamy (Retd) & Anr v. Union of India & Ors, 2018) (Chugh & Raghavan, 2019). The usage of Aadhaar has been restricted by the Supreme Court to particular circumstances, and usage by private actors has been severely restricted. This does not align with the current vision of NODEs which appears to seek a high degree of private sector participation.

Second, Aadhaar authentication failures have now been well-documented. These failures can have exclusionary consequences and need to be addressed before they become the sole option for citizens to authenticate themselves. There have been several studies that have demonstrated the deficiencies of biometric-based Aadhaar authentications in the case of welfare delivery (Khera, 2017). Recent studies in Jharkhand show that the requirement of biometric-based Aadhaar authentication increased transaction costs for the average beneficiary of the Public Distribution System (PDS), and reduced benefits received by the subset of beneficiaries who had not previously registered an ID by 10%. Furthermore, the deletion of suspected "ghost" beneficiary accounts led to cancellation of a significant number of real beneficiaries (Muralidharan, Neihaus, & Sukhtankar, 2020). While the benefits of efficiency may be realised in full or in part, this shift may have some unintended consequences that create either transitional or permanent exclusion. Another study in Jharkhand has shown that beneficiaries face challenges in accessing pensions because of friction in the process of linking bank accounts with Aadhaar cards (Dreze & Khera, 2016).

While there have been critical architectural issues that have manifested over time (Khera, 2019), the most significant concern is with grievance redressal. Nodal agents and functionaries responsible for the delivery of services are often unable to understand or explain the cause of failures as they often do not know what the error codes stand for or where they can be remedied.

Digital vulnerability is a risk any digital ecosystem is susceptible to in the absence of appropriate notification mechanisms. The Aadhaar infrastructure has also seen several security threats over the years. Current mechanisms are designed to recognise only incidents with demonstrated impact and not to address vulnerabilities in early stages of the crisis. This can have grave implications specially in a

country like India whose record at handling private data has not been spotless as evidenced by the leak of Aadhaar data over the years (Vidyut, 2018).

The White Paper does not provide any comprehensive protocols to address these pre-existing problems of the Aadhaar infrastructure which is envisioned as the basis for service delivery NODEs. Multiple online and off-line modes of authentication should be allowed for users to have a wide choice of methods to share credentials. Other digital systems such as Self-Sovereign Identities (SSI) could also be considered in addition to existing mechanisms for identification for service delivery on NODEs.

5. NODEs can pose risks to competition and systemic stability.

Our analysis of digital infrastructures in the financial sector suggest that the design and data flows of these infrastructures have far reaching consequences for competition in the market and systemic stability in addition to individual users' privacy (Raghavan, Chugh, & Singh, 2019). The broad objectives of NODEs will become unattainable unless regulatory frameworks for NODEs address these risks.

5.1. NODEs can pose a risk to competition in the market.

While the impact of largescale digital infrastructures like NODEs on markets is still being understood, it is clear that the design of these infrastructures will influence markets and competition within them. These may drive healthy competition among entities that may not have previously competed. For instance, several products have been created to enable digital payments through the UPI infrastructure but three very different entities currently have the largest market share: PayTM (a Payments Bank, previously an e-wallet), GooglePay (a BigTech company) and PhonePe (an Indian fintech) (Dvara Research, 2020). On the flip side, there is potential for these infrastructures to erode existing infrastructures or markets (Mazer, 2018). For instance, the impact of the proposed Public Credit Registry (PCR) on credit bureaus and the developing credit information markets in India is unclear (Chugh & Raghavan, 2019), and evidence of the impact of their interaction from other countries is mixed (Policy and Economic Research Council, 2018).

5.2. NODEs can pose a risk to systemic stability.

The security of large data infrastructures has been a major source of concern in recent years. Reports of data security issues in crucial public infrastructures (including the Aadhaar system) as well as breaches of large private infrastructures (such as data breaches of Equifax, the credit reporting agency) have revealed their vulnerabilities. Interdependencies between market players and market infrastructures, could cause IT risks to escalate into systemic crises especially if some firms do not have expertise or experience in managing such risks (Basel Committee on Banking Supervision, 2018). Centralisation of data also raise the risks of a single point of failure, creating the need to consider alternative strategies for aggregation. Finally, compromises of data in one database can have implications for the data quality

in related or linked databases. These concerns must be addressed as they strike at the heart of the benefits that large data-sharing systems have to offer.

Other countries have addressed this challenge by enacting new laws, by empowering competition regulators to check abuse of dominance or by constituting cross-sector/cross-regulator supervisory bodies with enforcement powers (Mazer, 2018). Such measures are necessary preconditions before NODEs can be considered.

II. Specific responses to Key Questions for Consultation presented in Chapter 7 of the White Paper

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

The White Paper identifies fifteen principles that provide standards for designing delivery platforms, creating "*transparent governance*" and building a "*vibrant community*" on NODEs. However, the underlying basis on which these fifteen principles have been opted is not clear. The principles appear to be suspended in a vacuum without being rooted in the objectives and purposes of NODEs.

In the absence of a clear foundational basis, there is a risk that the guiding principles will be interpreted and moulded in ways that suit self-interests of different participants. This conflict of interest can threaten the safety and effectiveness of NODEs. The White Paper needs to clearly articulate the core objectives of these principles to prevent this possibility. This concern has been set out in more detail in this response, in the overarching comments at Section I.1 (page 1) above.

In particular, reference can be made to the Gemini Principles which are also cited by the White Paper (Centre for Digital Built Britain, 2018). The Gemini Principles (see Box 2, on page 7) are rooted in three core objectives i.e. (i) having a clear purpose (ii) being trustworthy and (iii) functioning effectively. The White Paper must incorporate similar core objectives to avoid ambiguity about the guiding principles. Similarly, the key "*mantras*" in the India Enterprise Architecture (IndEA framework) cited in the White Paper i.e (i) citizen-centricity (ii) outcome-focus (iii) standardisation (iv) reusability and (v) integration could serve as a reference for the same (Ministry of Electronics and Information Technology, 2018).

Further, the following guiding principles in the White Paper in particular create a variety of concerns in NODEs:

i. Principle 1 (*Be Open and interoperable*);
ii. Principle 4 (*Ensure security and privacy*);
iii. Principle 5 (*Adopt an agile, data-driven development method*);
iv. Principle 6 (*Define accountable institutions*); and
v. Principle 8 (*Create transparent data governance*).

The concerns with these principles are set out in detail below.

(i) Principle 1: Standards of openness defined in the White Paper are unclear.

Principle 1 in the White Paper requires delivery platforms to be open and interoperable through open standards, licenses, databases, APIs etc. The White Paper defines "*open*" (in footnote 1, page 6 of the White Paper) as

"*principles of openness including but not limited to transparency, accessibility, interoperability, open APIs and standards and open source code, where appropriate*". This definition is caveated by "*it must be noted that each NODE will have its own configuration and degree of 'openness', which may introduce certain limitations in order to adhere to specific objectives, context or to mitigate potential risks*".

This definition is ambiguous and disregards the well-developed definitional clarity in the open-source software community regarding open-source standards and their application. This can lead to "open-washing" where proprietary and strongly protected software is incorporated into delivery platforms in the guise of "open" software (Kodali, 2020), affecting transparency, accountability and auditability of NODEs. Software used for building public service delivery platforms must be open source by default, with exceptions only when clearly articulated.

(ii) Principle 5: Adopting an agile, data-driven development method creates concerns for user protection.

Principle 5 for NODEs (on page 16 of the White Paper) advocates the adoption of an agile and data-driven development method where

"*Instead of spending upfront time to build a solution incorporating all value-added features… build incrementally by developing MVPs to which additional features are added as our understanding of user behaviour improves and/ or new use cases emerge. Regularly review data about the performance of the system and leverage analytics to identify new features and capabilities that can improve its user-centricity and effectiveness.*"

While this method can conserve resources for building and operating NODEs, it creates serious concerns for user protection.

Learnings from the United Kingdom's Universal Credit Program suggest that such agile, data-driven "*test and learn*" approaches make users vulnerable to harms and exclusion at scale. Further, these effects may converge more onto users from low-income or marginalised groups with low digital access whose use of services and feedback might not loop back to service providers (Special Rapporteur on extreme poverty and human rights, 2019). While the White Paper's emphasis on feedback mechanisms is welcome, it should not adopt "*test and learn*" as a core guiding principle for large scale public infrastructure where the State is accountable to citizens who suffer the harms of such an approach.

(iii) Principle 6: Private entities should not be given accountability for the overall administration of NODEs.

Principle 6 (on page 17 of the White Paper) requires NODEs to have a single point of accountability and to identify

"*an accountable institution for each delivery platform, whether a public or a private body or a coalition set up as a Special Purpose Vehicle (SPV) or Public Private Partnership (PPP), which is responsible for the overall administration of the platform and setting the standards or rules of engagement that drive accountability. Finally, organization structures, platform resourcing and performance management all need to align with these frameworks.*"

Private entities should not be given sole power and accountability for the overall administration, setting the standards and rules of engagement of NODEs. This concern has been set out in more detail in this response, in the overarching comments at Section I.3 (page 10) above and is summarised again for convenience.

Entities that are set up as a point of accountability must make sure that the higher order concept of openness based on transparency, access, participation, and democracy are enforced as much as possible (Schlagwein, Conboy, Feller, Leimeister, & Morgan, 2017). However, private entities may be driven by incentives that do not necessarily align with the principles of the NODEs framework. Principle 6 appears to be opening up the option for institutions that are not accountable to the public to be handling and accessing troves of citizens' information from Government and undertaking public service delivery without being subject to the accountability requirements of public sector institutions such as audits, compliance with the Right to Information Act, etc.

Further, competitive and institutional neutrality in regulation are indispensable for promoting competition in the market. Private entities on NODEs, however, may be inclined to impinge on these principles by creating self-serving rules of engagement or by entrenching their own technology and software as standards for the delivery platform. This can lead to unaccountable private entities gaining control over licensing of technology and software that process all citizens data, potentially violating the principle of openness (Principle 1) also aspired to by NODEs.

There should be clearly prescribed protocols for procuring technology services[4] and inviting participation from private entities on NODEs. The governance of NODEs must be held up to the level of accountability required from all public institutions in terms of audit, oversight and transparency.

(iv) Principle 8: Outlining data policies and standards on ownership is not preferable.

Principle 8 in the White Paper (on page 18) encourages transparent data governance i.e. outlining "*data policies and standards on ownership, contribution and consumption of data.*"

It is not appropriate to outline standards on ownership of personal data because the legal paradigm of property ownership has severe shortcomings in the context of personal data. In any event, following the

[4] Some of these protocols are prescribed in the India Enterprise Architecture, the "Policy on Adoption of Open Source Software for the Government of India", and in the "Policy on Open Application Programming Interfaces (APIs) for Government of India".

Privacy judgment, in India personal data and informational privacy (linked to the sharing of personal data) are now protected as fundamental rights and therefore they are akin to human rights entitlements which cannot be simply traded or "bought" and "sold" between Government and private sector.

In any event, several complications and logical inconsistencies arise by treating personal data under traditional ownership paradigms, including those set out below.[5]

i. It is difficult to establish singular ownership of personal data. In most cases, personal data is produced as a result of relationships with others and therefore, it is difficult to exercise property rights over such personal data (Solove, 1972).
ii. Personal data is not always alienable from the person to whom it belongs, as in the case of property (movable, immovable or intangible intellectual property) which can be transferred to a third party by alienating property or licensing IPR. This is not possible in case of personal data which will remain tied to the person to some degree (Samuelson, 1999).
iii. Personal data cannot be treated strictly as "creations" of a person.
iv. Treating personal data as IPR can invent an artificial scarcity in personal data (Liebenau, 2016).
v. Information asymmetry between persons, instant gratification and fear of or denial of service can impair a person's choice about alienating or licensing their personal data. Extending ownership paradigms to personal data may therefore be inconsequential to individuals who in effect are under duress to hand over "property" if they need access to a service (Baron, 2012) (Prins C., 2006).

NODEs should continue to offer constitutional protections to the user's right to privacy over their personal data under Article 21 of the Constitution. NODEs should focus on these constitutional protections instead of creating new paradigms for personal data.

2. For principles (either individually or collectively), are there platforms (in India or globally) that you consider as benchmarks (from a best practice standpoint)?

The design of NODEs should be informed by local and where relevant, global experiences. Lessons can be learnt from cases where there have been instances of grave failures even in the most efficient adoption of digital ecosystems. This concern has been set out in more detail in this response, in the overarching comments at Section I.4 (page16) above that are summarised again for convenience.

First, a push for digital-by-default policies can lead to a system of exclusion-by-design. The digital-by-default approach works on the premise that all users are online and digitally skilled. Such an approach can have adverse implications for the poor and more vulnerable users in India who do not have proper access to digital interfaces.

[5] *Legal Constructs of Personal Data*, Malavika Raghavan, Dvara Research (forthcoming publication).

Second, governance failures in digital infrastructure can impose high economic and social costs on government and users. A lack of transparency in the creation and functioning of digital infrastructure creates room for lots of corruption. Further, lapses in cybersecurity of the digital infrastructure and personal data leaks can have an adverse impact on users.

Third, interconnected databases can lead to technology failures at scale. Interlinking different databases in India through NODEs without being conscious of extant data quality issues can create major issues for the users and the government.

Finally, co-opting private entities to build and operate public digital infrastructure without following proper procedures can lead to high costs, adverse incentive misalignments and failure in fulfilling objectives.

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

Three types of concerns could potentially arise when migrating from existing infrastructure to NODEs: (i) legislative and regulatory concerns (ii) financial concerns, and, (iii) operational concerns.

(i) Legislative and regulatory concerns

Legislative concerns arise from the lack of a law backing the creation of NODEs' and its subsequent interlinkage to other databases. The Supreme Court's ruling in the Privacy judgment (Justice K.S. Puttaswamy (Retd) & Anr vs Union of India & Ors., 2017) and subsequently the Aadhaar Judgment (Justice K.S. Puttaswamy (Retd) & Anr v. Union of India & Ors, 2018) mandate that the use of individuals' personal data such as that in the creation of NODEs and the interlinkage of individuals' databases must satisfy the three-part test set out in the Privacy Judgment.

To this end, the involvement of private entities in public service delivery and their access to personal data from Government must be carefully calibrated especially given clear bright lines drawn after the Aadhaar judgement. This concern has also been set out in more detail in this response, in the overarching comments at Section I.2 (page 8 onwards) above.

(ii) Financial concerns

Financial concerns emerge from the multi stakeholder model envisioned in NODEs. Inadequate incentives (both financial and non-financial) for even a single stakeholder may adversely impact the functioning of the NODE platforms as well as user's experience. Inadequate incentives can often encourage rent-seeking among participants, ultimately increasing the costs that users must bear to avail of the infrastructure (Anognya & Gupta, 2020). This concern has been set out in more detail in this response, in the overarching comments at Section I.3 (page 10) above as well.

(iii) Operational concerns

Operational Concerns in migrating from existing Govtech infrastructure to NODEs can arise from digital-by-default strategies set out in more detail in this response, in the overarching comments at Section I.4 (page 16 onwards) above. They can also create concerns for competition and other systemic risks as set out in Section I.5 (page 21 onwards) above and summarised again for convenience:

i. Digital-by-default design can exclude large swathes of population from public service delivery, considering the limitations users face in accessing digital interfaces effectively.
ii. They can increase opacity and corruption. Indian experience suggests that digitisation without considering local power structures and political economy among other factors can heighten vulnerability and create room for corruption. Section 4.2 (at page 17) discusses this in greater detail.
iii. Interconnected databases can lead to technology failures at scale. Various government departments collect data for distinct purposes and collect different information under the same headings (Wright, Abraham, & Shah). Interlinking different databases via NODEs without being conscious of these challenges can adversely affect citizens' entitlements. This is discussed in greater detail in Section 4.3 (at page 18).
iv. Lapses in cybersecurity can render users more vulnerable to economic and data harms, as seen in many reported breaches of the Aadhaar system over the years (Vidyut, 2018) (Kodali, 2017).
v. NODEs must consider authentication mechanisms in addition to Aadhaar to avoid exclusion due to the prevailing issues in Aadhaar. The Supreme Court has also severely restricted private sector's use of Aadhaar, reinforcing the need to consider other authentication mechanisms.
vi. NODEs can pose a risk to competition in the market. The creation of large-scale infrastructure does not guarantee an improvement in the competitiveness of the market. A decision to create a NODE must be informed by the impact it will have on existing infrastructures in the sector.
vii. NODEs can pose a risk to systemic stability. Cybersecurity vulnerabilities in large scale infrastructure can escalate into systemic risks given their interface with a large number of participants. It can also adversely affect the quality of the data in the system as a whole.

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

The definition of "open" is ambiguous in the White Paper. The term cannot be understood without very clear explanations of the technical standards and their application in designing delivery platforms. This can lead to "open-washing" where proprietary and strongly protected software are incorporated into delivery platforms in the guise of "open" software (Kodali, 2020). Public service delivery platforms on NODEs should be built on open source software. This concern has been set out in the overarching comments at Section I.3.3 (page 1510) above and are summarised again for convenience.

Open source software can engage a wider community of stakeholders such as security experts and researchers without any limitations created by proprietary software. Further, open source licenses can allow communities to create highly tailored solutions to meet the specific needs of that community. This can help participants in NODEs to create a diverse set of solutions to various problems that they experience in their respective sectors.

Open source codes allow greater visibility into the functioning of the code and promotes auditability. This can help public authorities to identify and address problems with a code expeditiously. Reference can be made to Estonia's Public Codes Registry which is based on open source technologies that allow complete visibility into the code. The Registry allows anybody to access and use the open source code unless there are compelling security reasons to not allow access (E-Estonia, 2019).

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

The NODEs framework aims to implement an 'ecosystem-based approach' to governance, as per the White Paper. Specifically, it envisages a community comprising private/commercial providers to use the personal data available through the NODEs framework.

As a public digital infrastructure, the creation and operation of NODEs must be pursuant to a governance framework that fulfils the three-part test set out in the Privacy judgment (Justice K.S. Puttaswamy (Retd) & Anr vs Union of India & Ors., 2017). First, the creation of NODEs will have to be backed by a suitable legislation. Second, that legislation must justify that the creation of bigger databases containing potentially richer, more sensitive personal information than that found in isolated datasets is necessary for pursuing a legitimate state aim. It will have to be proven on merits that NODEs are necessary for pursuing a legitimate state aim. Third, the legislation will also have to demonstrate that the creation of NODEs is proportionate to the specified purpose and least intrusive.

Further, future legislation that could allow the creation of NODEs cannot legitimise a blanket interlinkage of subsequent databases. Each interlinkage of databases needs to fulfil the necessity and proportionality tests, as held in the Aadhaar judgment (Justice K.S. Puttaswamy (Retd) & Anr v. Union of India & Ors, 2018).

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

Alongside PPP models or community crowdfunding models, data ecosystems globally have considered (i) taxation on the industry (ii) membership fees for participants on the data ecosystem and (iii) data usage fees (Mazer, 2018).

While the NODEs framework may adopt any of these financing models it deems fit, it must be ensured that private entities do not completely control delivery platform(s) on NODEs. Private entities should not have sole power and accountability for the overall administration of NODEs in the interests of regulatory and competitive neutrality, and accountability to citizens of India whose personal data they will be acquiring from the Government and handling.

Further, care should be taken to ensure that the incentives driving public entities and private entities are aligned with each other. Inadequacy of financial and non-financial incentives can discourage private entities from engaging with NODEs, or alternatively encourage them to create perverse incentives such as charging end-users excessively (Gupta, 2020) (Anognya & Gupta, 2020). These concerns have been set out in the overarching comments at Section I.3 (page 1010) above.

7. 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?

NODEs can expose users to severe harms related to data privacy and exclusion. A strong governance framework which includes clear redress mechanisms for individuals and incorporates strong institutional accountability and audit are required to protect users against these harms.

(i) NODEs have the potential to expose users to severe kinds of exclusion and data privacy-related harms.

These concern have been set out in the overarching comments at Section I.4 (page 1610) which deals with the risks that arise for citizens, and are summarised again below for convenience.

Using digital infrastructure for service delivery can lead to exclusion even in highly sophisticated societies. In NODEs, the emphasis on service delivery via digital platforms and digital touchpoints automatically excludes a major section of the Indian population that is not savvy with using digital technology. This includes vulnerable classes of users such as low-income users and historically marginalised users. Further, NODEs rely on Aadhaar-based services and existing last-mile infrastructure for service delivery. The existing exclusion problems with Aadhaar and the high costs involved in using last-mile service providers like BCs and CSCs increases the risk of exclusion (Gupta, 2020) (Anognya & Gupta, 2020). In this context, building new digital infrastructure without addressing existing problems in service delivery may not reduce exclusion but in fact potentially widen it.

Second, NODEs can create several risks to user privacy. Any restriction of the right to privacy should fulfil the three-part test set out in that judgement to be valid. Building and operating NODEs without fulfilling this test will amount to an infringement of the fundamental right to privacy.

(ii) **Strong governance frameworks are necessary for NODEs to protect users against exclusion and harm.**

These solutions have been set out in the overarching comments at Section I.2 (page 810) and Section I.3.2 (page 12) which set out elements which need to back up the governance framework for any proposals like NODEs. These are summarised again for convenience. The creation of NODEs will have to be backed by a suitable legislation that fulfils the three-part test in the Privacy judgement. The legislation will also have to demonstrate that the creation of NODEs is proportionate to the specified purpose and least intrusive. Further, future legislation that could allow the creation of NODEs cannot legitimise the blanket interlinkage of subsequent databases. Each interlinkage of databases needs to fulfil the necessity and proportionality tests, as held in the Aadhaar judgment, to be constitutionally valid (Justice K.S. Puttaswamy (Retd) & Anr v. Union of India & Ors, 2018).

Further, any entity involved with NODEs will handle and access troves of citizens' information from Government and undertaking public service delivery. Consequently, they must be subject to the accountability requirements of public sector institutions such as audits, compliance with the Right to Information Act, etc. Publicly accountable institutions must lie at the heart of the Governance framework any such system of NODEs. Failure to ensure this could set back the transparency and accountability of NODEs in its current form (and Principle 6 of the Guiding Principles in the White Paper must be re-considered as a result). Not ensuring public accountability could also lead to private entities gaining control over licensing of technology and software that process all citizens data and to undertake public service delivery, potentially violating the principle of openness (Principle 1) also aspired to by NODEs.

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

There may be several ways in which NODEs can mobilise the wider community to develop innovative solutions. One of the ways is the usage of open-source software, as highlighted in our response to question 4 in the White Paper, above (on page 28 of this document).

Further, community engagement and public accountability will be required from entities involved with NODEs. To this end, the involvement of private entities in public service delivery and their access to personal data from Government must be carefully calibrated especially given clear bright lines drawn after the Aadhaar judgement. Care should be taken to ensure that the incentives driving public entities

and private entities are aligned with each other. These matters have been set out in the overarching comments at Section I.3 (page 1010).

Further, usage of open-source software which allows inspection of source code is critical to community engagement of developers and is also aligned with the principle of openness. Relying on proprietary software of private entities to build delivery platforms or provide solutions/services on NODEs can lead to vendor lock-in, create opacity, limit engagement and thwart creative innovative solutions. Public service delivery platforms must be built on open source software.

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

A strong grievance redress model is one key aspect of driving user engagement and trust, which can improve adoption. A good complaints handling process must lie at the heart of such an expansive infrastructure, and detailed recommendations for the design of such a system are set out in response to Key Question 10 below.

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

Key principles and a relevant model for a grievance have been set out in the overarching comments at Section I.3.2 (page 1210). We have set out in page 12 (and summarise again below) the elements of a grievance model that must be at the heart of such an expansive infrastructure that will impact so many citizens and have so many entities performing a variety of functions and operations. Poor systems can harm our most vulnerable and voiceless, so the need for a simple and accessible grievance system that reinforces accountability is essential for the legitimacy of any such large digital project.

A relevant blue-print for a unified redress agency— Financial Redress Agency (FRA)—for the financial sector exists in the Report of the Financial Sector Legislative Reforms Commission (FSLRC) (Financial Sector Legislative Reforms Commission, 2013). The Financial Redress Agency (FRA) was proposed in the FSLRC to simplify redress in the financial sector which has "*multiple laws and regulated by multiple agencies covering various sectors*" (Financial Sector Legislative Reforms Commission, 2013). The FRA was envisaged to provide a consumer-facing front-end at the district level where complaints regarding all financial products can be registered. Following registration, the FRA would channel the complaint to the appropriate regulator, and entity in the backend through technology-intensive processes for resolution via mediation and light-weight adjudication (Task Force on Financial Redress Agency, 2016).

Such a sector-neutral grievance redressal structure would considerably reduce the burden on users to identify the points of liability, identify the regulator/ entity and then lodge a complaint. NODEs must provide unified grievance redressal front-end at the local level like the FRA with effective back-end adjudication processes to provide users easy access to effective grievance redress. This would adopting such a grievance redressal mechanism will be beneficial for NODEs in fulfilling its own objectives of:

i. *Single touchpoint for users*: NODEs seeks to provide a single touch-point for users for interacting with public and private provider entities. Creating a single touch point for grievance redressal would further this objective.
ii. *Strong feedback loops*: NODEs will have to (a) understand the challenges that are impeding operations (b) identify and mitigate risks of harm to the user and (c) identify gaps in regulation so that they can gain traction and mobilise a wider community of participants. A unified front-end for grievance redressal like the FRA for NODEs will be able to serve as an effective feedback loop that can analyse user complaints and highlight weakness in the ecosystems. Further, the unified front-end agency can be required to publish periodical reports of grievances raised and actions taken to ensure transparency.

Customer helpline numbers can be one of the means through which users can access the unified grievance redressal front-end of a NODEs. In addition, users should be allowed to ask for redress via written letters or e-mail, fax, telephone, missed call services, online portals, mobile apps, SMS and video to significantly improve access to this grievance redressal front-end (Task Force on Financial Redress Agency, 2016). The grievance redressal mechanism should also provide users visibility into the grievance redressal process by allowing online as well as offline tracking of their complaints for transparency (Dvara Research, 2018).

11. Imagine designing a NODE in the context of the state or sector that you work in (please refer to Figure 4 and the Figures in Section 5), and describe–

11.1. The key challenge/ problem your NODE is seeking to address? What benefits will it offer?

11.2. The key building blocks for this node or key components of the delivery platform? Please list any challenges / barriers you may face in building this platform e.g., poor data quality, data is in silos, lack of common open standards and APIs, transition from legacy systems, etc. and how you may overcome these

11.3. With reference to the 5 design principles on "Governance", please indicate what the governance model could look like for your NODE. What are some challenges/ barriers you may face in establishing a successful model e.g. inter-departmental coordination and strategies to overcome these?

11.4. The "Community" for your NODE – key stakeholders, how would they engage with the platform and build on top of it? What benefits would having a vibrant community offer

and what additional use cases can be unlocked? Please list any challenges (e.g. incentivising adoption, value sharing) and how you may overcome these?

The overarching comments as well as the specific comments to the questions in the White Paper in this response have been written from the perspective of financial inclusion which we are associated with. Please see the concerns in the overarching comments at Section I. 4 (page 1610) in particular regarding the exclusionary consequences that can result from context-blind design of digital infrastructures in India. Given our unique demographic profile, digital divide and quality of ICT infrastructure it is important to engage with more organisations dealing with concerns of lower-income consumer and citizens, and these citizens themselves who are the majority of our country.

12. Are there any useful resources that you have come across that would help the broader community, as we build out this NODE approach?

The NODEs framework can consider Self-Sovereign Identities (SSI) as one additional alternative for Aadhaar for digital credential management and authentication for service delivery on NODEs. As noted in our overarching comments at Section I.4.5 (page 20) above, online and off-line modes of authentication should be allowed for users to have a wide choice of methods to share credentials.

The SSI architecture works on a system of peer-to-peer agents. These peers (hardware components, usually computers) are responsible for forming relationships between components of the system. The relationships are important for the different components to establish trust between each other. The network of SSI architectures has three main peers; these are *credential issuers*, *credential holders* and *credential verifiers*.

i. *Credential issuers* could be anybody who has the authority to issue credentials such government agencies, banks, educational institutions or employment agencies. A credential issuer can verify whether they have issued a particular credential, whether such a credential has been tampered with and if such a credential is valid and has not been revoked (Windley, 2019b).

ii. *Credential holders* are the owners or the individuals who own the credential that has been issued and use it to validate their identity across different contexts (Windley, 2019b).

iii. *Credential verifiers* in a given context are agents who require validation of an individual's identity. For example, if an individual wants to apply for a loan at a bank, the bank will want to verify the identity of the applicant as well as their employment status, income and asset ownership. In this case, the loan-providing bank is the credential verifier.

These three peers in combination ensure that the issuers issue credentials that can be validated, holders determine the credential they need to make assertions about themselves and verifiers determine which credentials are acceptable and which issuers are trustable (Windley, 2019a). For examples, for getting

access to customised farming advisory at the start of the seeding season, or right before harvest time, a farmer should be able to own and use their personal information credential in a manner that automatically verifies their identity, and is only able to access information about the location of their farm (and no other details that are not required for the context of advisory services), and suitably provide advisory based on the geographic and climatic conditions of the location. Accordingly, it is submitted that self-sovereign identity systems can be considered in addition to other existing means of identification in the country.

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

Not applicable.

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

MeitY must publicly release all responses to consultation received to provide for open and transparent communication of the issues highlighted across the market. This is in furtherance of best practices as already employed by regulators such as the Telecom Regulatory Authority of India.[6] Further, we welcome any opportunity to present our views or respond to questions and comments on our research to MeitY through individual consultations, workshops or through any other means deemed appropriate.[7]

[6] *See* https://main.trai.gov.in/release-publication/consultation.
[7] The corresponding author for this publication can be contacted at srikara.prasad@dvara.com.

References

[OAIC] Office of Australian Information Commissioner. (2017). *Australian Community Attitudes to Privacy Survey.* OAIC. Retrieved from https://www.oaic.gov.au/assets/engage-with-us/research/acaps-2017/acaps-2017-report.pdf

AlMarzouq, M., Zheng, L., Rong, G., & Grover, V. (2005). Open Source: Concepts, Benefits, and Challenges. *Communications of the Association for Information Systems, 16*, 756-784. Retrieved from https://pdfs.semanticscholar.org/c5d0/67eb6d1eaa2f6d89dd6584778f144f3fe739.pdf?_ga=2.230225496.535020421.1585318744-474830801.1563176062

Anognya, P. (2020, January 13). *Does Co-opting Private agents for welfare delivery work?* Retrieved from Dvara Research: https://www.dvara.com/blog/2020/01/13/does-co-opting-private-agent-for-welfare-delivery-work/

Anognya, P., & Gupta, A. (2020, March 11). *The 'Common Services Centre' Model: A no-win scenario?* Retrieved from Dvara Research: https://www.dvara.com/blog/2020/03/11/the-common-services-centre-model-a-no-win-scenario/

Baker, S. (2014, July 30). *Obamacare Webiste Has Cost $840 Million*. Retrieved from The Atlantic: https://www.theatlantic.com/politics/archive/2014/07/obamacare-website-has-cost-840-million/440478/

Baron, J. B. (2012). *Property as Control: The Case of Information*. Retrieved from www.repository.law.umich.edu/cgi/viewcontent.cgi?article=1017&context=mttlr

Basel Committee on Banking Supervision. (2018, February). *Sound Practices: Implicatins of fintech developments for banks and bank supervisors.* Retrieved from Bank for International Settlements: https://www.bis.org/bcbs/publ/d431.pdf

Benjamin, S., Bhuvaneswari, R., Rajan, P., & Manjunatha. (2007, January). *Bhoomi: 'E-Governance', Or, An Anti-Politics Machine Necessary to Globalise Bangalore?* Retrieved from Casum-m: https://casumm.files.wordpress.com/2008/09/bhoomi-e-governance.pdf

Business Line. (2018, January 31). *Implementation of C-KYC may prove a tough task.* Retrieved from Business Line: https://www.thehindubusinessline.com/markets/stock-markets/ckyc-implementation-may-prove-a-tough-task/article9553960.ece#

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

Chadha, T. (2019, October). Literacy in India: The Gender and Age Dimension". *ORF Issue Brief No. 322, Observer Research Foundation*. Retrieved from https://www.orfonline.org/wp-content/uploads/2019/10/ORF_IssueBrief_322_Literacy-Gender-Age.pdf

Chugh, B., & Raghavan, M. (2019, June 18). *The RBI's proposed Public Credit Registry and its implications for the credit reporting system in India*. Retrieved from Dvara Research: https://www.dvara.com/blog/2019/06/18/the-rbis-proposed-public-credit-registry-and-its-implications-for-the-credit-reporting-system-in-india/

Chugh, B., Raghavan, M., & Singh, A. (2019, April). *Primer on Designing Optimal Regulation.* Retrieved from Dvara Research : https://www.dvara.com/research/conference2019/wp-content/uploads/2019/04/Primer-on-Designing-Optimal-Regulation.pdf

Citizens Advice Flintshire. (2018, September). *Citizens Advice Flintshire Submission to the United Nations Special Rapporteur for Extreme Poverty & Human Rights.* Retrieved from United Nations Human Rights Office of the High Commissioner: https://www.ohchr.org/Documents/Issues/EPoverty/UnitedKingdom/2018/NGOS/CitizensAdviceFlintshire.pdf

Dreze, J., & Khera, R. (2016, June 28). *Recent Social Security Initiatives in India*. Retrieved from SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2800699

Dvara Research. (2018, October 10). *Comments to the Ministry of Electronics and Information Technology (MeitY) on the draft Personal Data Protection Bill 2018, dated 27 July 2018, submitted by the Committee of Experts on a Data Protection Framework for India.* Retrieved from Dvara Research: https://www.dvara.com/blog/wp-content/uploads/2018/10/Response-to-draft-Personal-Data-Protection-Bill_DvaraResearch.pdf

Dvara Research. (2020, March 12). Comments to the Reserve Bank of India on the Draft Framework for Authorisation of a Pan-India New Umbrella Entity (NUE) for Retail Payment Systems dated 10 February 2020. Retrieved from Dvara Research: https://www.dvara.com/research/wp-content/uploads/2020/03/Dvara-Research-Response-to-RBI-NUE-Framework.pdf

E-Estonia. (2018, May). *What we learned from the eID card security risk?* Retrieved from E-Estonia: https://e-estonia.com/card-security-risk/

E-Estonia. (2019, April). *Estonia creates a public code repository for e-governance solutions*. Retrieved from E-Estonia: https://e-estonia.com/code-repository-for-e-governance/

Financial Sector Legislative Reforms Commission. (2013, March). *Report of the Financial Sector Legislative Reforms Commission.* Retrieved from Department of Economic Affairs, Ministry of Finance, Government of India: https://dea.gov.in/sites/default/files/fslrc_report_vol1_1.pdf

Government Digital Service. (2017, February 9). *Government Transformation Strategy.* Retrieved from Government Digital Service: https://www.gov.uk/government/publications/government-transformation-strategy-2017-to-2020/government-transformation-strategy

Gupta, A. (2020, January 21). *Reaching the Last Mile: Delivery of Social Protection in India*. Retrieved from Dvara Research Blog: https://www.dvara.com/blog/2020/01/21/reaching-the-last-mile-delivery-of-social-protection-in-india/

Henriques-Gomes, L. (2020, March 26). *Robodebt: government admits it will be forced to refund $550m under botched scheme*. Retrieved from The Guardian: https://www.theguardian.com/australia-

news/2020/mar/27/robodebt-government-admits-it-will-be-forced-to-refund-550m-under-botched-scheme

High Level Committee on Deepening of Digital Payments. (2019, May 17). *Report of the High Level Committee on Deepening of Digital Payments.* Retrieved from Reserve Bank of India: https://m.rbi.org.in/Scripts/PublicationReportDetails.aspx?UrlPage=&ID=922

High-level Task Force on Public Credit Registry. (2018, April). *Report of the High-level Task Force on Public Credit Registry.* Retrieved from Reserve Bank of India: https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/PCRRR09CF7539AC3E48C9B69112AF2A498EFD.PDF

Information System Authority. (2018, May 14). *Estonia Offers Recommendations in the Light of eID Vulnerability*. Retrieved from Information System Authority, Republic of Estonia: https://www.ria.ee/en/news/estonia-offers-recommendations-light-eid-vulnerability.html

Jordan, A. J., & Turnpenny, J. R. (2015). *The Tools of Policy Formulation: Actors, Capacities, Venues and Effects.* Cheltenham, United Kingdom: Edward Elgar Publishing. Retrieved from https://www.econstor.eu/bitstream/10419/182379/1/978-1-78347-704-3.pdf

Justice K.S. Puttaswamy (Retd) & Anr v. Union of India & Ors, W.P (Civil) No 494 of 2012 (The Supreme Court of India September 26, 2018). Retrieved from https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_26-Sep-2018.pdf

Justice K.S. Puttaswamy (Retd) & Anr vs Union of India & Ors., W.P. (Civil) No. 494 of 2012 (The Supreme Court of India August 24, 2017). Retrieved from https://www.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf

Karp, P. (2019, November 22). *'Pay the money back': robodebt, the Coalition's backflip and how it 'hounded' welfare recipients*. Retrieved from The Guardian: https://www.theguardian.com/australia-news/2019/nov/22/pay-the-money-back-robodebt-the-coalitions-backflip-and-how-it-hounded-welfare-recipients

Khera, R. (2017, December 16). Impact of Aadhaar on Welfare Programs. *Economic & Political Weekly, 52*(50).

Khera, R. (2019, April 6). Aadhaar Failures: A Tragedy of Errors. *EPW Engage, 54*(14). Retrieved from EPW Engage: https://www.epw.in/engage/article/aadhaar-failures-food-services-welfare

Kodali, S. (2017, December 5). *A billion users, but no big reporting policy*. Retrieved from Medium: https://medium.com/karana/a-billion-users-but-no-bug-reporting-policy-20ce35122795

Kodali, S. (2018, August 1). *The Technology Apocalypse*. Retrieved from Medium: https://medium.com/the-fifth-elephant-blog/the-technology-apocalypse-3b5090f835ea

Kodali, S. (2020, March 19). *How do we build India's National Open Digital Ecosystem?* Retrieved from Medium: https://medium.com/hasgeek/how-do-we-build-indias-national-open-digital-ecosystem-f7ffe73bd1e

Kumar, A. (2020, January 3). Who Is The State?: Reconsidering Article 12 In The Context Of Common Service Centres. Retrieved from Live Law: https://www.livelaw.in/columns/reconsidering-article-12-in-the-context-of-common-service-centres-151223?infinitescroll=1

Liebenau, D. (2016). *What Intellectual Property Can Learn from Informational Privacy, and Vice Versa*. Retrieved from SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2842447

Lipowicz, A. (2011, October 17). *OPM says USAJobs fixed, but complaints continue*. Retrieved from FCW: The Business of Federal Technology: https://fcw.com/articles/2011/10/17/opm-usajobs-working-users-disagree.aspx

Mazer, R. (2018, June). *Emerging Data Sharing Models to Promote Financial Service Innovation: Global trends and their implications for emerging markets.* Retrieved from Amazon AWS: s3-eu-central-1.amazonaws.com/fsd-circle/wp-content/uploads/2018/07/12111727/Emerging-Data-Sharing-Models-to-Promote-Financial-Service-Innovation-June-2018-Mazer.pdf

Ministry of Electronics and Information Technology. (2020, March 17). *Strategy for National Open Digital Ecosystems Consultation Whitepaper*. Retrieved from Medianama: https://www.medianama.com/wp-content/uploads/mygov_158219311451553221l.pdf

Ministry of Electronics and Information Technology. (2018, May). *India Enterprise Architecture Framework.* Retrieved from Ministry of Electronics and Information Technology, Government of India: https://negd.gov.in/sites/default/files/IndEAdocument.pdf

Mithun, M. (2019, December 20). *Why Telangana farmers are facing the brunt of the new digitised land record system*. Retrieved from The News Minute: https://www.thenewsminute.com/article/why-telangana-farmers-are-facing-brunt-new-digitised-land-record-system-114462

Moore, T. (2013, August 15). *'Worst failure of public administration in this nation': payroll system*. Retrieved from The Sydney Morning Herald: https://www.smh.com.au/technology/worst-failure-of-public-administration-in-this-nation-payroll-system-20130807-hv1cw.html

Muralidharan, K., Neihaus, P., & Sukhtankar, S. (2020). *Identity Verification Standards in Welfare Programs: Experimental Evidence from India*. Retrieved from National Bureau of Economic Research: https://ideas.repec.org/p/nbr/nberwo/26744.html

Open Source Initiative. (2007, March 22). *The Open Source Definition*. Retrieved from Open Source Initiative: https://opensource.org/osd

Pathways for Prosperity Commission. (2019). *Lessons from Aadhaar: Analog Aspects of Digital Governance Should Not Be Overlooked.* Retrieved from retrieved from: https://pathwayscommission.bsg.ox.ac.uk/sites/default/files/2019-09/lessons_from_aadhaar.pdf

Pickert, K. (2014, July 30). *Report: Cost of HealthCare.Gov Approaching $1 Billion*. Retrieved from Time: https://time.com/3060276/obamacare-affordable-care-act-cost/

Policy and Economic Research Council. (2018, March). *The Case for a Public Credit Registry in India: Additional Evidence for Consideration.* Retrieved from Durham: Policy and Economic Research Council: https://www.perc.net/wp-content/uploads/2018/03/India_PCR.pdf

Prins, C. (2006). Property and Privacy: European Perspectives and the Commodification of our Identity.

Raghavan, M., Chugh, B., & Singh, A. (2019, April 4). *Primer on Consumer Data Infrastructure*. Retrieved from Dvara Research: https://www.dvara.com/research/conference2019/wp-content/uploads/2019/04/Primer-on-Consumer-Data-Infrastructure.pdf

Sabatier, P., & Mazmanian, D. (1980, January). The Implementation of Public Policy: A Framework of Analysis. *Policy Studies Journal, 8*(4), 538-560.

Samuelson, P. (1999). *Privacy as Intellectual Property?* Retrieved from University of California at Berkeley: http://people.ischool.berkeley.edu/~pam/papers/privasip_draft.pdf

Schlagwein, D., Conboy, K., Feller, J., Leimeister, J. M., & Morgan, L. (2017). Openness With and Without Information Technology: A Framework and a Brief History. *Journal of Information Technology*, 297-305.

Solove, D. J. (1972). *Understanding Privacy.* Cambridge, Massachusetts: Harvard University Press.

Special Rapporteur on extreme poverty and human rights. (2019, April 23). *Visit to the United Kingdom of Great Britain and Northern Ireland: Report of the Special Rapporteur on extreme poverty and human right.* Retrieved from United Nations : https://undocs.org/pdf?symbol=en/A/HRC/41/39/Add.1

Tanfani, J. (2013, December 2). *Technology failures grow all too common in government projects*. Retrieved from Los Angeles Times: https://www.latimes.com/nation/la-xpm-2013-dec-02-la-na-government-computers-20131202-story.html

Task Force on Financial Redress Agency. (2016, June). *Report of the Task Force on Financial Redress Agency.* Retrieved from Department of Economic Affairs, Ministry of Finance, Government of India: https://dea.gov.in/sites/default/files/Report_TaskForce_FRA_26122016.pdf

The Hindu. (2017, August 16). *Centre's eBiz initiative stutters.* Retrieved from The Hindu Website: https://www.thehindu.com/business/Economy/centres-ebiz-initiative-stutters/article19498323.ece

The Sydney Morning Herald. (2016, April 4). *Queensland Health payroll fail: Government ordered to pay IBM costs*. Retrieved from The Sydney Morning Herald: https://www.smh.com.au/technology/queensland-health-payroll-fail-government-ordered-to-pay-ibm-costs-20160404-gnxpqj.html

Van Meter, D. S., & Van Horn, C. E. (1975, February 1). The Policy Implementation Process: A Conceptual Framework. *Administration & Society*, *6*(4), 445-488.

Victoria Legal Aid. (2019, December 9). *Robo-Debts*. Retrieved from Victoria Legal Aid: www.legalaid.vic.gov.au/find-legal-answers/centrelink/robo-debts

Vidyut. (2018, May 4). *#AadhaarLeaks- A continuously updated list of all Aadhaar data leaks*. Retrieved from Medianama: https://www.medianama.com/2018/05/223-aadhaar-leaks-list/

Windley, P.J. (2019a, May 1). *An overview of Self-Sovereign Identity: the use case at the core of Hyperledger Indy.* Retrieved from Hyperledger: https://www.hyperledger.org/blog/2019/05/01/an-overview-of-self-sovereign-identity-the-use-case-at-the-core-of-hyperledger-indy

Windley, P.J. (2019b, August). *Life-Like Identity: Why the Internet Needs an Identity Metasystem.* Retrieved from Phil Windley's Technometria: https://www.windley.com/archives/2019/08/life-like_identity_why_the_internet_needs_an_identity_metasystem.shtml

World Bank Group. (2019). *Open Source for Public Goods.* Retrieved from World Bank Group: http://documents.worldbank.org/curated/en/672901582561140400/pdf/Open-Source-for-Global-Public-Goods.pdf

Wright, G. P., Abraham, S., & Shah, N. (n.d.). *Report on Open Government Data in India.* Retrieved from Centre for Internet & Society: https://cis-india.org/openness/publications/ogd-report