The Internet Democracy Project welcomes the consultation by the Ministry of Electronics and Information Technology, Government of India on the Strategy for National Open Digital Ecosystems 2020 and would like to thank you for this opportunity to present our comments on this important policy document.

At the Internet Democracy Project (https://internetdemocracy.in/, http://genderingsurveillance.in), we work towards realising feminist visions of the digital in society, by analysing power imbalances in the areas of norms, governance and infrastructure in India and beyond, and providing proposals for alternatives that can lead to a more equal digital society for all.

We greatly appreciate the Ministry's effort vis-à-vis drafting a strategy for a technology driven e-governance ecosystem at this early stage. This practice has been fairly uncommon among technology regulators, as tech policies are often drafted after the technology has been developed and implemented, leading to a regulatory vacuum that allows state and non state actors to misuse their authority. We particularly appreciate the attempt to identify principles for both technology and non-technology elements. Again, too often the latter are only an afterthought. The White Paper signals an important change in both regards. In the interest of a transparent process, we hope that all responses will be made public.

While we greatly appreciate these efforts, we do believe, however, after closely studying the paper, that it is essential to take a step back before we move forward. In particular, before developing the details of the NODE framework, it is important that we make sure its fundamentals are strong. For the moment, this is not the case. In a nutshell, while the White Paper claims to aim for a citizen-centric approach, the approach currently developed in the White Paper would only further the growing power imbalances between citizens on the one hand and the state and corporations on the other hand that the age of datafication has brought with it. A truly citizen-centric approach needs to prioritise citizens' concerns continuously, rather than mixing them with attempts to address the private sector, and even government interests as well.

For this reason, before developing detailed answers to the questions asked in the White Paper, we believe clarity needs to first be shed on these fundamental concerns. We do that in part I of this submission. In part II, we will then comment on the principles proposed in the White Paper specifically, against the backdrop of these aforementioned fundamental concerns.

PART I. FUNDAMENTAL CONCERNS

We would like to draw your attention to the following fundamental concerns:

- **Ambiguous terms**

The paper uses various vague and ambiguous terms making it difficult to know exactly what is being discussed, and thus to understand and comment on whether the proposals made are appropriate or how they could be strengthened and improved.

For example, while the paper defines 'NODEs' as delivery platforms that transform societal outcomes, it doesn't define the kinds of services or products that it considers essential to such transformation. In some cases, the reference explicitly is to the delivery of public services (e.g. p. 9). But elsewhere, including in most of the examples provided, it is clear that the intention is to ensure that private actors who are profit-driven will benefit from these platforms as well.

This is additionally problematic because the paper fails to identify concretely the 'significant economic, social and governance benefits for a country such as India' (p. 13) that it claims the introduction of NODEs would bring about. It also hides from view the fact that different outcomes (e.g. social and economic) cannot necessarily be achieved simultaneously, or might require very different approaches that do not necessarily sit easily with each other. The definitions included do not provide any sense of the priorities proposed.

Such slippages and ambiguities can therefore mislead stakeholders on what really is aimed for as well as causing confusion.

In addition, some terms in the White Paper have already been defined in other policies; however, the White Paper does not seem to have taken into consideration these existing definitions, and has instead proposed new ones without delineating the reason for deviance.

For example, the term 'open' has been defined in other policies, such as the 'Policy on Adoption of Open Source Software for Government of India'.[1] This policy does not merely define 'openness' as opening the source code. It also provides that the source code shall be available for the community/adopter/end-user to study and modify the software and to redistribute copies of either the original or modified software. Further, the source code shall be free from any royalty' (p. 3). The definition of the term 'open' in the NODE White Paper, however, only includes opening the source code (see p. 6). It does not include principles such as the ability to modify the software and to redistribute copies of either the original or modified software. Further, the paper does not propose uniform principles of openness, but advocates that each NODE will have its own degree of openness.

[1] Policy on Adoption of Open Source Software for Government of India, 2014.

In the light of the above, it is suggested that **terms used should be clear and unambiguous**. Further, the drafters should **delineate clearly in the policy drafts reasons to diverge from the existing policies and regimes**.

- **Questions of Utility**

This White Paper argues that there is a need to revisit the existing system of governance. In order to achieve this, the White Paper prescribes NODEs, an ecosystem-based approach composed of interoperable platforms that will enable different parts of the government system (across ministries and departments) to collaborate for service delivery as well as allowing private players to build new services and solutions on top.

While the intent of improving governance is welcomed, the White Paper, however, neither identifies the concrete concerns vis-à-vis existing systems of governance that undermine citizens' ability to access services and entitlements, nor does it explain how NODEs will be able to address each of these concerns.

Where concerns and solutions are not clearly matched, it is unlikely that the NODE framework as currently proposed will in fact be able to achieve the desired outcomes. General statements in this regard are not sufficient. At the same time, the risk of, perhaps unintended, outcomes that are undesirable from the perspective of the citizen (such as deeply intensified dataveillance) increases considerably.

Thus, it is suggested that before deliberating over the framework of NODEs, **there should be a deliberation and consultation regarding the purpose, utility and ability of a NODE.**

- **What is the priority of NODE: economic development or social welfare?**

The above is further exacerbated as the White Paper seems to confuse and conflate the economic goals of the nation with its development agenda.

For example, on p. 9 of the White Paper, it is stated that for India to become a $5 trillion economy by 2024, there is a need to 'improve the access, quality, efficiency and effectiveness of the delivery of public services'. The White Paper then continues: 'NODEs can enable service delivery in ways that were previously not possible; by reinventing market models to create greater access for underserved populations, offering better pricing or cost-effectiveness in the delivery of public services, and lowering transaction costs and inefficiencies.'

Thus, the White Paper seems to presume that market models in the delivery of services will automatically achieve the nation's development agenda, that initiatives driven by economic parameters necessarily improve social development outcomes. However, there is no evidence that this is necessarily the case. The private sector generally requires a profit incentive to cater to the public interest. Social transformation tools such as NODE thus often do not ensure optimum models for private entities. The White Paper does not recognise this. Moreover, the White Paper also fails to foresee and provide a framework to ensure sufficient market competition among private delivery platforms. If only one private entity is providing a service, the dependence of the government and populace on that entity increases and it may seek higher prices for the same services, exploit consumers, or lower service standards due to its monopoly.

More generally, while development may boost the economy, social and economic goals cannot necessarily be achieved through the same route, and economic growth does not necessarily translate into similar increases in social well-being. Kerala serves as a remarkable example: while it is not the most advanced state economically, it is the most socially developed state in India. In contrast, high-income states such as Andra Pradesh do much worse than Kerala in terms of social well-being.[2]

Such an approach is not surprising seeing the great emphasis the Government of India has put on the economic value of data as an asset for the country in other draft policy documents, including drafts, in recent years.[3] But rather than presuming that the market route is the best way to address the needs of the public, the White paper should have **laid out the alternatives, and explained for each (including the market model) why the approach is or isn't desirable** for the citizen-outcomes NODEs are supposed to achieve. Neither the White Paper nor other government documents have engaged in detail in this exercise so far.

- ## Citizen-centric service delivery platforms, require a recognition that data is social

While this White Paper claims to aim at building interoperable technology-driven systems for governance that are citizen-centric, it seems to advocate an approach that only furthers the deep datafication of individuals and their lives that we have seen over the past decade or two. As we have outlined elsewhere,[4] such an approach is based on a dominant understanding of data as a resource, and in this case, the sole fuel for enabling service delivery as well as for 'unlocking solutions' (see e.g. p. 5).

- ### *Faith in a 'single source of truth' is a fallacy*

In a democracy, this approach towards individuals and governance is disconcerting. Instead of putting citizens at the heart of these structures, these mechanisms fragment individuals and reduce them to data points that are privileged over the presence and context of their physical bodies and lives. This approach is exemplified by the description of data registries in the paper as a 'single source of truth' (see p. 7).

[2] Kapoor, Amit (2017, October 23). Social Progress India Launches Social Progress Index: States of India 2017. *Social Progress.* https://socialprogress.in/2017/10/social-progress-india-launches-social-progress-index-states-of-india-2017/

[3] See e.g. the draft National e-Commerce Policy, 2019, and the Economic Survey, 2018-2019.

[4] Kovacs, Anja and Ranganathan, Nayantara (2019, November). Data Sovereignty, of Whom? Limits and Suitability of Sovereignty Frameworks for Data in India. *Data Governance Network* Working Paper 03. Mumbai. https://internetdemocracy.in/reports/data-sovereignty-of-whom/

What this disregards is that in reality, data is social, and thus always subject to interpretation.[5] Where conflicts of interpretation exist and the marginalised do not have avenues to argue their case because systems are being automated, evidence indicates that it is often they who lose out.[6] The many instances in which people who need entitlements the most have lost out on them because of Aadhaar-related authentication and other problems are only one example.[7]

Similar problems have also been observed, e.g., where land titles have been digitised. Although the aim of such exercises ostensibly is to establish clear titles, in practice, research from Karnataka has found, for example, that they disembedded existing heterogenous tenure forms 'to re-imbed new ones', transforming control over both property and economy in the process. Those who lose out in the process are frequently those already most vulnerable.[8]

- *More data does not necessarily lead to better decision-making*

The social nature of data is also one reason why the collection of ever more data in the name of 'truth' does not necessarily lead to better data-driven decision making, as the White Paper seems to hold on p. 9 and elsewhere. For example, during the COVID19 pandemic, there has been plenty of evidence that the need for identity documents prevented many people from getting access to food that they desperately needed.[9] Despite the data being available, the policy has not been changed. Data-driven decision making does not only require data to be available, but also the will to act on it, even when what it teaches us might not be what was hoped for. In other cases, the data gathered may not be the right data, or incomplete, and for that reason lead to faulty decision-making.

Thus, if NODE is to be a genuinely citizen-centric framework, **the interests of the citizens should be at the heart of every aspect of the proposed NODEs ecosystem**. This means, among other things, that the framework for the ecosystem ensures that **where there is disagreement about what constitutes 'the truth', a citizen has an easy route to recourse**. No citizen should be excluded from the services or benefits they are entitled to because of such disagreements.

Improving service delivery or driving surveillance capitalism?

- *Facilitating the exploitation of citizens as resources*

[5] Kovacs, Anja (2020, 28 May). When Our Bodies Become Data, Where Does That Leave Us? *Deep Dives.* https://deepdives.in/when-our-bodies-become-data-where-does-that-leave-us-906674f6a969

[6] Sriraman, Tarangini (2018). *In Pursuit of Proof: A HIstory of Identification Documents in India*. New Delhi: Oxford University Press.

[7] Khera, Reetika. (2019, April 6). Aadhaar Failures: A Tragedy of Errors. *Economic & Political Weekly*. https://www.epw.in/engage/article/aadhaar-failures-food-services-welfare

[8] Benjamin, Solomon and Raman, Bhuvaneswari (2011). Illegible Claims, Legal Titles, and the Worlding of Bangalore. Revue Tiers Monde, 206, 37-54. https://www.cairn.info/revue-tiers-monde-2011-2-page-37.htm#

[9] Khera, Reetika and Somanchi, Anmol. (2020, April 25). COVID-19 and Aadhaar: Why the Union Government's Relief Package is an Exclusionary Endeavour. *Economic & Political Weekly*. https://www.epw.in/engage/article/covid-19-and-aadhaar-why-union-governments-relief

Ignoring the social nature of data is not the only problem in the White Paper where its claims to the centrality of the citizen are concerned. In addition, the approach proposed seems to allow for the exploitation of citizens as resources for wealth-creation. This move is not dissimilar to the manner in which land in developing countries was appropriated by colonial powers for many centuries.[10] In this case, however, it is citizens targeted by the state and private corporations of their own country.

The sale of the Vahan and Sarathi database data by the government to private actors has already been criticised widely in this context, and it has been pointed out how this could put minorities in particular at risk.[11] Similarly, proposals included in the White Paper to share data with, for example, insurers do not necessarily benefit citizens - this is a case that has to be made, and will likely require far stricter checks and balances to be put into place. Research from the United States, for example, has shown how access to ever more granular data by insurers has actually made those already vulnerable even more so.[12] The belief that sharing citizens data with private actors will automatically lead to good is a deep fallacy, even where that data is supposedly 'anonymised'.

- *The move towards surveillance capitalism*

In addition, where the White Paper argues that NODE provides the potential for 'unlocking solutions', this 'unlocking' is presumely also based on the intense datafication of Indian citizens' bodies, lives and behaviour, and the provision of access to such data to a wide range of actors. After all, if we are not yet aware of what these solutions would entail (and what problem they would address), such unlocking will likely require the use of data provided by citizens for purposes not initially intended or foreseen by them.

And precisely because it is not clear what such solutions would help to resolve exactly and whether the gains for citizens actually outweigh the costs, this is a dangerous exercise. The datafication of people's bodies and lives to facilitate the resource extraction that allows other actors to create 'value addition' after all is precisely what is at the heart of surveillance capitalism.[13] Seeing that these dynamics are based on the exploitation of human beings, state governance should not replicate or even facilitate them.

If it is hard to escape the impression that the White Paper seems to allow for precisely such exploitation, and through it the furthering of surveillance capitalism in India, this is also because of the central role that private actors seem to play in each aspect of the NODE ecosystem's development and implementation. While the seamless delivery of government services to citizens might be the main goal, it appears that the private sector will not only be

[10] Zuboff, Shoshana. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. London: Profile.

[11] Singh, Varun. (2019, 10 July). Govt selling vehicle and DL data of Indians for Rs 3 crore, 87 private companies already bought it. *India Today.* https://www.indiatoday.in/auto/latest-auto-news/story/govt-selling-vehicle-and-dl-data-of-indians-for-rs-3-crore-87-private-companies-already-bought-it-1565901-2019-07-10; Mukherjee, Sreemoyee. (2020, 6 March). How Poor Data Protection Can Endanger Communities During Communal Riots. *The Wire.* https://thewire.in/rights/vahan-database-protection-riots

[12] O'Neil, Cathy (2016). *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens* Democracy. London: Allen Lane.

[13] Zuboff, Op. Cit.

allowed to build ‘on top of’ the infrastructure that will be provided, but will also be central to the development of that infrastructure as such: the ‘delivery platform’ and the ‘community’ or not as separated as they are made out to be. But an overlap or alignment of interests of citizens, and the private sector cannot be presumed. Such a dual involvement creates conflicts of interests that, while perhaps creating considerable windfalls for the private sector, have potentially devastating consequences for citizens.

Thus, if **the interests of the citizens are to genuinely be at the heart of every aspect of the proposed NODEs ecosystem**, this also means that the ecosystem and its framework are framed in such a way that **individuals are not reduced to resources for wealth creation by other actors and thus exploited**. And it means that the nature of the relationship between a service provider and user in the system should be duly noted: **considering that the bargaining power is strongly in favour of the service provider, policies must delineate robust checks and balances** for service providers (or fiduciaries), whether state or private actors.

- Security, surveillance and discrimination

The proposal in the White Paper to recognise data registries and exchanges as the single source of truth is concerning for an additional reason. This proposal is reminiscent of the Chinese model of identification and governance, wherein individuals are assessed on the basis of their smart cards, which are tied up to practically every transaction that they make. This is problematic as it requires the interlinking of a large number of data reservoirs and centralisation of data, which risks becoming a tool for surveillance. Especially in the absence of any meaningful reform of the intelligence services and data protection legislation, such registries may lead to further exclusion of already marginalised communities within the social fabric of India. It also poses a national security threat.

The White Paper, on p. 34, does recognise that these practices may lead to weaponisation of delivery platforms or data; however it does not delineate any concrete responses to mitigate these potential risks.

Therefore, **data registries should be decentralised** and should be maintained separately for particular purposes, they should **follow the principles of data minimisation** and should be composed of **only necessary data for the mentioned purposes**. **Strong data protection and other laws guaranteeing citizens’ rights should be put into place** before developing the infrastructure.

- Technology is not a solution in itself, it is a means

Linked to several of the above problems is that the White Paper seems to perceive technology as a magic potion. It proposes a paradigmatic shift to a technology-driven governance ecosystem based on interoperable digital delivery platforms, without a clear outline of the problems this would resolve (or potentially create) in each instance. In doing so, it poses technology as the ultimate solution.

Past experiences have already illustrated the shortcomings of such visions. For example, the White Paper once again presumes that a reduction in leakages will be a benefit for citizens and governments that will automatically result from implementing the NODE ecosystem (see p. 9). But while similar assumptions were made and disproved with regard to Aadhaar, research has shown that these expectations were not borne out in reality.[14]

Another assumption that has proven to be dangerous is that seamless service delivery can be enabled without human involvement or interference. For example, GSTN (the Goods and Services Tax Network), although cited by the White Paper (see p.5) as an empowering tech solution that increases the ease of doing business, suffers from innumerable problems, including the following: 1) the system server does not have enough capacity in comparison to the load; 2) the system does not allow to revise returns once filed; and 3) the local officers have been granted with hardly any rights to resolve technical issues faced by businesses.[15] All these concerns exacerbate the many challenges faced by businesses, rather than resolving them. This is especially true for smaller businesses, for whom the fact that the network is completely only and a human contact point is thus absent, has often proven an insurmountable challenge.

Solutions driven solely by technology also generally fail to take into account the social, economic and political realities of a society. Again, Aadhaar has been one such example. Although it was supposedly launched to ensure seamless delivery of essential services, it ended up excluding many of those marginalised as it failed to consider the concerns of people with disabilities, lack of infrastructure, and lack of access to electricity, among others.[16]

In this light, it is recommended that **technology solutions should be considered as means to an end (seamless governance), but not an end** in themselves. They should **respond to a clear and well-defined problem statement**, and there should be **clarity on why they are the best way to address this problem**. In addition, there should always be offline alternatives to governance systems and humans should be involved in critical decision making.

PART 2. ADDITIONAL COMMENTS ON THE NODE GUIDING PRINCIPLES

What the above amounts to then, is that the guiding principles for the NODE's currently provided by the White Paper themselves need a guiding framework of values that ensure, rather than presume, the centricity of the citizen. Without this, the guiding principles alone are not sufficient to enable a seamless NODE that can facilitate a genuinely citizen-centric transformation of the nation.

[14] Dreze,Jean, Khalid, Nazar Khera,Reetika, and Somanchi, Anmol. (2017, 16 Dec) Pain without Gain? Aadhaar and Food Security in Jharkhand.*Economic & Political Weekly*. https://www.epw.in/journal/2017/50/special-articles/aadhaar-and-food-security-jharkhand.html

[15] Sharma, Umesh. (2020, 31 March). 57 Technical Glitches and Issues of GSTN. *TaxGuru*. https://taxguru.in/goods-and-service-tax/technical-glitches-issues-gstn.html

[16] Khera, Op. Cit, fn 7.

It is thus with the above comments in mind that we make the following additional comments on some of the principles proposed in the White Paper:

Principle 1, be open and interoperable, is imperative to build an interoperable technology driven ecosystem for governance. As it not only ensures efficiency, competition and safeguards from monopolies, it instills trust in the systems. Open source softwares also enable participation of the public in reporting security, and privacy threats.

While this paper recognises the importance of this principle, as noted above it fails to acknowledge the three existing national policies in line with this principle: the National Policy on Information Technology, 2012; the Policy on Adoption of Open Source Software for Government, 2014; and the Framework on Adoption of Open Source Software in E-Governance Systems, 2015. Each of these policies emphasise the adoption of open source standards and values. In fact, the Policy on Adoption of Open Source Software for Government, 2014, states that the 'Government of India shall endeavour to adopt Open Source Software in all e-Governance systems implemented by various Government organisations, as a preferred option in comparison to Closed Source Software (CSS).'

In contrast to this, the White Paper advocates that each NODE will have its own degree of openness (see p. 6). As mentioned above, even the definition of the term 'open' is not comprehensive in the White Paper, as it fails to highlight characteristics of the principle of openness such as the ability to modify the software, to redistribute copies of either the original or modified software and to distribute source code without any royalty.

Seeing that openness is central to the National Open Digital Ecosystems, the definition of 'open' should be in line with these existing government policies. In addition, a transparent oversight board should be set up to decide what should be the degree of openness of a NODE, and the reasons for its decisions should be made available in public domain.

While **principle 2, make reusable and shareable,** is a good principle as such, an impact assessment should be conducted before systems are actually reused and shared. Moreover, a standard or condition should be incorporated that a model can only be reused and repurposed when it has met with clearly-defined parameters of success, or when there is sufficient evidence to show that it can meet with such success subject to modifications for which standards have also been laid out.

Principle 4, ensure security and privacy, will obviously have to be central to any digital ecosystem that is developed, but it isn't clear at the moment what is understood by this. There is reference to data purpose specification, collection limitations, and user consent frameworks, as well as to the ability for users to restrict and revoke access. But would that mean that the sale by the Government of Vahaan and Sarathi data, unlikely to have been suspected by an user, would no longer be allowed?

While registering your vehicle and obtaining a driver license are both legally required, it is not clear on what grounds this sale by the Government to third parties, including those who are in a position to monetise this data, was justified, whether in anonymised or identifiable form.

The matter here is not simply one of whether people should have the choice to opt-out, but whether this is a practice the Government should engage in in the first place. Until a comprehensive data protection legislation with strong protections of citizens' rights is passed in India, building such comprehensive, interlinked digital systems is therefore not recommended.

These concerns are also related to **principle 8**, on **transparent data governance**, which advocates for 'data policies and standards on ownership, contribution and consumption of data'. Apart from the fact that it is not clear what ownership, contribution and consumption mean in this context, or who would be the relevant actors for each, such policies and standards cannot change with each initiative that is being taken. Thus, again, a comprehensive data protection legislation is essential before initiatives like this can be built out.

Perhaps it does already deserve to be pointed out, however, that the concept of data ownership is not an appropriate one to secure citizen's rights in the digital age.[17] Also, it deserves to be noted that in the example on state services delivery in the White Paper, there is an explicit proposal to open state NODEs and data to the private sector. This might well fundamentally undermine the relationship of trust between the citizen and the state, as well as undermine any protections of their data against private interests that a future data protection law might give citizens.

As noted in the first part of this submission, concerns regarding the increased surveillance capacity that NODE enables need to be addressed where principles 4 and 8 are concerned as well, including through legislation to reform India's intelligence agencies and through strong data protection legislation.

Where **principle 5, adopting an agile, data-driven development method**, is concerned, again a number of questions arise. Which principles drive how decisions about data collection and interpretation are made? Promoting a 'fail fast' culture might work in some cases, but can also put citizens at tremendous risk, at the expense of 'unlocking solutions' and 'innovation'. In fact, such an approach might at times work for for-profit initiatives that private corporations want to build on top of the technology and to which users have to opt-in. It is hardly appropriate for the delivery of essential services to citizens, as per their entitlements.

Similarly, for **principle 14, be analytics-driven and learn continuously**, too, a framework of direction needs to be put in place to guide what needs to be learned and what the goals of any analysis will be. Here as elsewhere, the interests of citizens, the government and private actors are not necessarily aligned. For the NODEs to contribute to citizen empowerment, prioritising citizens interests in asking questions of and analysing data is essential.

[17] Tisné, Marting (2018, 14 Dec). It's Time for a Bill of Data Rights. *MIT Technology Review*. https://www.technologyreview.com/2018/12/14/138615/its-time-for-a-bill-of-data-rights/; Zuboff, Op. Cit.

The way it is defined at present, **principle 6, defining accountable institutions**, leaves open space for private bodies to not only become the supposed point of accountability (while consumer rights remain rather weakly enforced in India), but will also be responsible 'for the overall administration of the platform and setting the standards or rules of engagement that drive accountability' (p. 17).. Leaving such an important function to a private body, or even to a mixed entity, leaves the door open for conflicts of interests that are likely going to work against citizens' interests and even have the potential to shift platforms' functioning away from their original objectives.

Similar concerns and questions are also relevant for **principle 15, enabling grievance redressal**.

Principle 7, establishing rules of engagement, would need to be done in such a way that citizens' interests are prioritised and that citizens can hold a public body accountable where that is not the case. Definitions of what 'fair' value sharing and 'undesirable behaviours' entail should also be provided and in line with citizens' interests.

Principle 10, adopt a suitable financing model, seems to prioritise finding a sustainable model. However, sustainability cannot be a prerequisite for a government-developed or facilitated citizen-centric platform, at least not from the outset. Even the example mentioned, OpenLMIS, was initially developed without a focus on sustainability. Where this is a priority from the start, the interests of citizens run the risk of being overrun by wider financial and commercial interests. The need for sustainability may override the value for citizens.

The achievement of **principle 11, ensure inclusiveness**, is central to the success of any governance framework that aims to empower citizens. It is noteworthy that while the White Paper does address the question of Internet access, it does not provide sufficient answers.

While it correctly highlights that Indian has the second-largest Internet user base in the world, it ignores the fact that nevertheless millions of Indians still do not have such access, let alone on a regular basis. And although it is true that the Aadhaar experiment has proven that even those without access can be integrated into such an ecosystem, it deserves to be asked to what extent that has actually been to their benefit. As noted earlier, for people without regular Internet access, finding recourse where problems relating to getting or using Aadhaar or updating their information arise, for example, has been even more of a challenge than for those who do enjoy such access - often with devastating consequences. The understandable lack of digital literacy of many of the unconnected only further compounds these problems.

Moreover, while it is laudable that the White Paper states that access should be affordable, it is difficult to see how that can be achieved for all from the outset. The current context already is rife with stories of people having to forego a day's wages because they are waiting for a connection at a ration shop for large parts of the day, so that their finger print authentication can go through.[18] A statement of intent to address such known problems alone sadly is not sufficient. The provision of IVRS services for users without smartphones could be helpful in

[18] See for example Sen, Jahnavi (2018, 26 Sep). In Rural Jharkhand, Aadhaar Link to Welfare Schemes Is Excluding the Most Needy. *The Wire*. https://thewire.in/government/jharkhand-aadhaar-pds-pensions

some cases, but likely will not be appropriate in all, and might end up excluding those most marginalised from a considerable number of the benefits that the platform is intended to provide.

These challenges are of relevance as well for **principle 12, facilitate participatory design and co-creation**, and **principle 13, drive end-user engagement**. Again, while these are laudable principles, in practice such engagements are frequently structured in such a way that those who participate are mostly from the more privileged sections of society. Frequently men, and sometimes those with a tech background, are overrepresented as well. Especially in light of the persistent deep inequalities in our country, in order to understand the challenges that the most marginalised in the country face, a focus on enabling their participation and understanding and centralising their challenges therefore has to be explicitly at the heart of this principle. Moreover, the differences among various marginalised groups, and their particular vulnerabilities, have to be taken into account in this as well.

Without such a conscious effort, 'collective' problem solving will merely amount to facilitating the interests of those whose voices are already heard the most (loudly).