Mozilla Corporation
331 East Evelyn Avenue
Mountain View, CA 94041

Mozilla's Comments in Response to the Public Consultation on India's Strategy for National Open Digital Ecosystems (NODE)

To

Ministry of Electronics and Information Technology (MeitY),
Government of India,
Electronics Niketan, 6, CGO Complex,
Lodhi Road, New Delhi – 110003

31 May 2020

We thank the Ministry of Electronics and Information Technology (MeitY) for the opportunity to provide feedback on the Strategy for National Open Digital Ecosystems (NODE)[1] (hereafter, "the Strategy" or "whitepaper"). We welcome the move to have a broad consultation by inviting suggestions from experts, stakeholders, and the general public and hope this approach is followed for future consultations by the Ministry.

Mozilla is a global community working together to build a better internet, with openness at the core of its functioning. As a mission-driven technology company, we are dedicated to promoting innovation and opportunity online. As our Mozilla and the Rebel Alliance report[2] highlights, there are over 22,000 contributors in over 49 open source projects managed by Mozilla. We are the creators of Firefox, an open source browser and the family of Firefox products, including Firefox Focus and Firefox Lite, as well as Pocket, used by hundreds of millions of internet users globally. Mozilla's commitment to user security and privacy is evident not just in our products but in our policies and in the open source code of our products.

According to the white paper, NODEs have been defined as 'open and secure delivery platforms, anchored by transparent governance mechanisms, which enable a community of partners to unlock innovative solutions, to transform societal outcomes'. Given our history as one of the largest and oldest open source projects in the world, we particularly appreciate the

[1] https://www.medianama.com/wp-content/uploads/mygov_1582193114515532211.pdf
[2] https://blog.mozilla.org/blog/2020/01/27/mapping-the-power-of-mozillas-rebel-alliance/

Mozilla Corporation
331 East Evelyn Avenue
Mountain View, CA 94041

pursuit of an 'open' framework and the broader goal of ensuring that openness is at the forefront of digital governance in India. It is equally reassuring that the white paper considers all digital infrastructure as a shared public resource, with 'sustainability and responsibility' as necessary prerequisites from the design stage of every project. The holistic implementation of these ideals will go a long way in ensuring that digital platforms remain citizen-centric while having transformative socio-economic impact.

However, the current white paper also leaves much to be elucidated on both the need and manner of implementation of such ecosystems before a national strategy can be finalized. In addition to a distinct lack of clarity on how governance mechanisms of NODEs would operate within existing and upcoming regulatory frameworks, the paper also creates the potential for 'open-washing' of projects.[3] The white paper leaves the definition of "open" vague and at the complete discretion of individual implementers. Consequently, implementers are not required to adhere to any minimum baseline of "open". This risks empowering private parties to develop closed ecosystems that are only open in appearance while being closed in practice. Illustratively, just a few targeted improvements could exponentially improve the Strategy and help it achieve its goal of ensuring citizen centric development:

1. One such move could be establishing a clear minimum baseline for "openness," guided by internationally accepted best practices and the Indian government's own policies. Adherence to this minimum baseline should be made a mandatory criterion for a project to be considered a NODE.
2. Secondly, the Strategy should explicitly recommend that strong data protection law with an independent data protection authority be enacted before any NODE project is implemented. Alongside rigorous internal data governance practices, this is the only way to ensure that NODE projects meaningfully protect the fundamental right to privacy that all Indians enjoy according to their Supreme Court.
3. The Strategy must also ensure that the principle that recommends exploring financing models contains an explicit list of prohibited practices and an illustrative list of principles to evaluate financing models against larger public interest concerns, grounded in data protection.
4. Finally, all outreach under a NODE project should be transparent, accountable, and inclusive. We recommend that MeitY hold at least one more generic public consultation with an improved white paper that addresses the concerns expressed by various stakeholders before proceeding onto next steps.

[3] https://openwashing.org/

Mozilla Corporation
331 East Evelyn Avenue
Mountain View, CA 94041

Despite these concerns, the white paper provides ample opportunity for constructive engagement and improvement of existing digital infrastructure projects in India. The clear emphasis placed on privacy, security, inclusive community building, and grievance redressal mechanisms, is a welcome move. Extending the open and consultative approach of this white paper to other stages of implementing the Strategy will be essential to creating real, positive impact. We look forward to sharing our experiences in maintaining some of the most widely used open source projects in the world throughout this process for this noble goal.

Warm regards,

Udbhav Tiwari,
Public Policy Advisor,
Mozilla Corporation

Jochai Ben-Avie,
Head of International Public Policy,
Mozilla Corporation

Chris Riley,
Director, Public Policy,
Mozilla Corporation

Mozilla Corporation
331 East Evelyn Avenue
Mountain View, CA 94041

Responses to Key Questions for Consultation

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.**

   In general, the guiding principles set out in Section 4 could be strengthened and further clarified by including specific and actionable criteria. These criteria can help evaluate whether a project meets the principle in both letter and spirit. Some specific feedback on the principles are provided below:

   A. **Principle 1 - Be Open and Interoperable:** The current principle leaves the definition of openness vague and subject to exploitation in the form of open washing. Open washing is when projects can call themselves open but do not exhibit any of the true characteristics of open projects. Many initiatives associated with the IndiaStack project have been accused of open washing,[4] and the leeway provided by the Strategy only increases the risk of this recurring.

      Mitigating possible open washing for projects under the Strategy will require the white paper and subsequent regulatory frameworks to define the minimum baseline of openness to be followed by these projects. Projects should be called 'open' only if they satisfy this baseline.

      As one example of a clear set of criteria to establish such a baseline, the Open Source Initiative (OSI) has a definition[5] and a useful list of licenses[6] that governs the classification of code and content as 'open'. Some of the criteria this baseline could include are:

      1. Free Redistribution of Software and Source Code - There should be no restriction on any party from selling or giving away the software and its source code as a component or in aggregated form.
      2. Derived Works - Modifications and derived works of the source code should be explicitly allowed.
      3. Must Not Restrict Other Software - Any other software that is distributed or utilized alongside the open NODE software should not be limited to open licenses.

[4] https://www.research.manchester.ac.uk/portal/files/102613332/FULL_TEXT.PDF
[5] https://opensource.org/osd
[6] https://opensource.org/licenses

Mozilla Corporation
331 East Evelyn Avenue
Mountain View, CA 94041

4. No Discrimination Against Persons or Groups - The software must not discriminate against any person or group of persons that intends to use it.

Contrary to common belief, this includes a wide variety of licenses that allow commercial use and accommodate the whitepaper's other criteria, such as 'value creation' across diverse stakeholders.

Additionally, there are many Indian government policies and documents[7] that can be excellent reference points for the government's own criteria for openness and also be used in the baseline. Some of the more prominent ones that the minimum baseline can utilize for different technical components of a NODE are:

Component	**Government Policy**	**Highlights of Policy Document**
Software	Policy on Adoption of Open Source Software for Government[8]	Definition of Open Source in Glossary. Explicit preference to OSS over closed source software.
Standards	Policy on Open Standards for e-Governance[9]	Mandates that all government e-processes adopt a "single and royalty-free open standard" in each technological domain.
APIs	Policy on Open Application Programming Interfaces (APIs) for Government of India[10]	Mandates APIs are published by all Government organizations for all eGovernance applications and Systems. Establishes a dedicated open API security cell.

[7] Non-Exhaustive List at https://cis-india.org/openness/files/economic-social-and-cultural-rights-in-india-foss/
[8] https://meity.gov.in/writereaddata/files/policy_on_adoption_of_oss.pdf
[9]http://egovstandards.gov.in/sites/default/files/Policy%20on%20Open%20Standards%20for%20e-Governance.pdf
[10] https://meity.gov.in/sites/upload_files/dit/files/Open_APIs_19May2015.pdf

Mozilla Corporation
331 East Evelyn Avenue
Mountain View, CA 94041

The Strategy should use these policies, along with OSI's definition, as reference points to create the minimum baseline criteria for 'open' projects. Failure to satisfy this minimum baseline should preclude a project from being a NODE and should disentitle it from having access to the Strategy's public and private benefits.

B. **Principle 3 and 5 - 'Be scalable' and 'Agile, data driven development':** Both of these principles could be improved by incorporating language that safeguards the public interest. This could happen, for example, by explicitly mandating that the scale of projects be evaluated not just in raw numbers but also against the impact of such scale on the fundamental rights of Indians at large.

C. **Principle 4 - Ensure privacy and security:** While the principle does include some very welcome and positive references on the importance of end-to-end encryption, it suffers from the same concerns as the principle on openness in that it is vague and subjective. The principle can be improved by including an all-encompassing provision that ensures all NODE projects, regardless of when they are launched, are compliant with India's data protection law (which should be enacted before finalizing the strategy).

D. **Principle 6 - Define accountable institution(s):** This principle can be reductive as it presumes that a single point of accountability is feasible for a modern, open, and community driven project. While legal and organizational structures are crucial in ensuring accountability, they cannot be a replacement for distributed ownership and valuing individual contributions, which can be harmed due to excessive centralization.

   For example, having the Unique Identification Authority of India (UIDAI) as the accountable institution for Aadhaar related concerns has not resolved the numerous[11] leakages that have resulted from poor implementation by partner government agencies and the private sector. The only way to effectively resolve such concerns is to simultaneously build the capacity of various players in this chain (state governments, statutory agencies, private players) while also ensuring that accountability is backed up by effective enforcement of rights and obligations. The principle could reflect this nuance by noting the inherent limitations of a single accountable institution approach and ensuring that it also points towards the importance of trust building and swift enforcement of accountability.

[11] https://www.bbc.com/news/world-asia-india-42575443

Mozilla Corporation
331 East Evelyn Avenue
Mountain View, CA 94041

E. **Principle 8 - Create transparent data governance:** The principle can better explicitly reference (apart from the example) the vital role that data protection laws play in meaningful data governance, both with regard to external liability and how data is treated within organizations.[12] As the Strategy rightly notes in the example of this principle, strong data protection laws are critical to effective and transparent data governance. As we have urged on numerous occasions in the past, adopting a national data protection law which provides for strong rights for users, strong obligations on those they entrust their data to, and strong enforcement through an empowered and independent regulator should be a national policy priority. Critically, in order for data protection law to fulfill this purpose, it must also apply to the State.

   The development of NODEs only further points to the need to adopt a national data protection law in order to give effect to this principle of data governance. The principle should reflect this reality as a minimal standard and on top of that should advocate for regular review of data ownership, contribution, and processing by independent parties (such as Data Protection Authorities) and security experts. The outcomes of such continuous monitoring should be made subject to independent oversight. This will also allow the project to use such outcomes to improve the project at a regular cadence.

F. **Principle 10 - Adopt a suitable financing model:** Given that NODE projects are painted as a shared public resource in the Strategy, it is vital that this principle caution against exploitative data processing, including selling data to private entities.[13] Rather than opening the possibility of projects chasing monetization via measures that sell data of Indians,[14] there should be a clear set of prohibitions when it comes to data processing. Some of these prohibitions could include:

   a. Selling personal data of users to third parties
   b. Making algorithmic decisions about users without human involvement
   c. Sharing data with any party (including government agencies) without informed and explicit consent

[12] https://pulse.microsoft.com/en/work-productivity-en/na/fa2-why-data-governance-matters-in-going-beyond-gdpr-compliance/
[13] Neha Alawadhi & Karan Choudhury, "Economic Survey Suggests Govt Can Monetize Citizen's Data as a
Public Good," Business Standard India, July 4, 2019,
https://www.business-standard.com/article/economy-policy/economic-survey-suggests-govt-can-monetise-citizen
-s-data-as-a-public-good-119070401558_1.html.
[14] https://www.hindustantimes.com/delhi-news/govt-clears-policy-to-sell-vehicle-registration-data/story-n4aBtGpJgETNuN9vbAW3LL.html

A separate set of principles that can be used to decide if the monetization harms privacy, security, or the larger public interest in any way. Internal teams within organizations and external agencies with independent oversight (such as data protection authorities) can use these principles when evaluating projects. Some of these principles, based on the 7 key principles present in the GDPR,[15] are:

a. Lawfulness, fairness and transparency: Is the monetization authorized in law, fair in how it treats user data, and transparent in explaining its functioning to users?
b. Purpose limitation: Is the use that the data is being subject to limited to the purpose for which it was originally collected?
c. Data minimization: Is the data being collected by the NODE purpose limited to the core function of the project rather than possible monetization opportunities?
d. Accuracy: Is the data that is utilized for monetization accurate and is the user allowed to question both direct and indirect inferences based on this data?
e. Storage limitation: Is data collected retained for the minimal time necessary exclusively for core functions of the project and possible future monetization potential?
f. Integrity and confidentiality (security): Does the monetization place user data at greater risk and by extension increase risk? (e.g., sharing it with third parties such as advertising brokers)
g. Accountability: Is the NODE project accountable for the direct and indirect harms that occur due to monetization of user data, including but not limited to, violations of data protection laws?

G. **Principle 11 - Ensure inclusiveness:** The principle should expand the scope of inclusivity to explicitly include accessibility, which is an integral part of many other government policies in related areas.[16] It should also explicitly state that NODEs should identify specific organizational staff who are responsible for, and held accountable for, examining the diversity, equity, and inclusion (DEI) within the project, the contributing community, and guarding end users interests at large.

[15] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/
[16]https://meity.gov.in/writereaddata/files/National%20Policy%20on%20Universal%20Electronics%281%29_0.pdf

Mozilla Corporation
331 East Evelyn Avenue
Mountain View, CA 94041

The development of NODEs also be appropriately diverse, equitable, and inclusive. MeitY can look to organizations such as Community Health Analytics Open Source Software (CHAOSS)[17] for both case studies and tools.

H. **Principle 15 - Enable grievance redressal:** While the explicit reference to grievance redressal is a positive move, the fact that most of these projects will be publicly funded requires them to have a much higher threshold for service delivery. It is vital to ensure that the constitutional and legal rights that guarantee access to critical government services are not replaced with internal mechanisms governed merely by standard operating procedures. The principle should explicitly highlight this and ensure that India's rich jurisprudence on this front applies appropriately to NODE projects.

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

The e-Estonia model referred to in the white paper, while not perfect and requiring a clearer articulation of the importance of a rights-based approach, does have many salient qualities when it comes to data governance and transparency. It is important to note the importance of clear, informed, and continuous consent for not just collecting but also the processing of data. Letting Indians own all their data (like the e-Estonia model) but not limiting what can be done with it by a NODE project will be counterproductive to the idea of privacy being a fundamental right. Another learning from Estonia that could be useful in this regard is the value of a strong data protection law with an empowered and independent DPA. The Estonian model also allows users to see the audit trail of any entity (including the government) which has accessed/processed their data and imposes significant sanctions for any access or processing of such data in an unauthorized way.

Exploring this model in greater detail in the next iteration of the white paper and explicitly carving out recommendations for the Strategy to adopt on data governance and user transparency from the e-Estonia model will help make it more secure and user-centric.

3. **What are the biggest challenges that may be faced in migrating from a 'GovTech' 1.0 or 2.0 approach to a NODE approach (e.g. inter-departmental systems integration, legacy systems modernization, poor usability, and poor data quality)? How might these be overcome?**

[17] https://chaoss.community/

Some of the biggest challenges that might be faced in migrating from a 'GovTech' 1.0 or 2.0 approach to a NODE approach are:

a. Lack of clarity on the applicability of existing laws, policies, regulations, and court decisions on NODE projects. Each NODE project should explicitly state the relevant policies, regulations, laws, and court decisions that apply to the project's operations and design. For projects of this nature, which propose to collect and process vast amounts of user data, a strong data protection law is critical. Unfortunately, India currently has no such law. It is vital that such a law is passed and be in force before projects under this Strategy are implemented. This would ensure that privacy is protected as a fundamental right rather than an amorphous privilege.

b. Merging data across silos may create additional security and privacy risks, especially due to legacy systems and poor cyber security practices. Upgrading infrastructure, incorporating best practices, and training personnel are effective methods for mitigating this problem. Purpose limitation, role-based access controls, and regular audits are all key means to mitigate many of these concerns as well.

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

See Response to Point A (Principle 1 - Be Open and Interoperable) in Question 1

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.

Yes, being shared resources that are publicly funded, all NODE projects should have a common governance framework in the form of modern laws and regulations passed by an independent legislature with judicial oversight over their functioning. Many of the criteria mentioned in the Principles in the Strategy (and in Question 1) should be explicitly enshrined in such laws. This includes data protection, security, accessibility, inclusion, transparency, community engagement, etc.

The absence of these protections will make projects open to the risk of regulatory capture, where private entities will have an overriding effect over existing public institutions or worse, can dictate the actions of these public institutions. In terms of structure, there should be baseline governance rules/regulations that apply to all NODEs along with some NODE-

specific governance policies and regulations that depend on the specific functions and kinds of data processed by that NODE.

It is also important to note that governance should be holistic and not be limited to laws and regulations. Internal corporate governance practices, community participation guidelines, specific policies for events that a NODE hosts, etc. are all examples of governance mechanisms that should be explicitly referred to in the Strategy and be an integral part of the roll out of any NODE project. Mozilla's own governance policies page can be a helpful reference point for what these could be in practice.[18]

Taking this holistic approach to governance and ensuring that the Strategy gives each stakeholder its due regard, building on rather than relying exclusively on government regulations and enforcement, will help ensure the Strategy remains people focused and rights centric.

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

Independent of the economics of funding, which other experts are better placed to answer, private financing or equity should not be used in a way that undermines oversight, accountability, or inclusion in projects that are public resources.

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?**

See Answer to Question 1, 3 and 5. Independently, the Centre for Internet and Society in India has also undertaken extensive research[19] into the harms that stem out of digital ecosystems that do not sufficiently account for human rights in India. Some of these are listed below:

a. Exclusion or loss of access because of technical failure, inaccurate information, or because of inaccuracies in the information that decisions are now based on
b. Undefined downstream harms as a result of repurposing of data and architectures

[18] https://www.mozilla.org/en-US/about/governance/
[19] https://cis-india.org/internet-governance/blog/big-data-in-governance-in-india-case-studies

c. Inability to seek redress as a result of automation of services or technical failure
d. Access to, and use of data, without consent
e. Unauthorized access as a result of a security breach
f. Vast digital profiles and lack of end user control
g. Lack of alternative options for accessing services
h. Monitoring
i. Discrimination

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?**

Mozilla is a radically open and participatory project[20] that has identified that the application of open practices[21] should always be paired with well-researched strategic intent. In practice, we enjoy a great diversity among the community structures of different Mozilla-driven open source projects, from Rust[22] to Thunderbird[23] to Firefox (there are actually multiple distinct Firefox communities)[24] and to others.

In order to improve internal practices and share our learnings with the world, we developed a set of basic models—"archetypes"—that projects could aim for, modifying them as needed, but providing a shared vocabulary for discussing how to think about any given project. We partnered with one of the leading authorities in open source, Open Tech Strategies,[25] in defining these archetypes.

The resulting framework consists of 10 common archetypes, covering things from business objectives to licensing, community standards, component coupling, and project governance. It also contains some practical advice on how to use the framework and on how to set up the project, all of which can positively inform the NODE strategy. The framework and these learnings can be found in our "Open Source Archetypes" report[26] with a quick summary of the 10 Archetypes mentioned in the document in the next page:

[20] https://medium.com/mozilla-open-innovation/being-open-by-design-deec6768706
[21] https://medium.com/mozilla-open-innovation/a-framework-of-open-practices-9a17fe1645a3
[22] https://www.rust-lang.org/en-US/community.html
[23] https://www.thunderbird.net/en-GB/
[24] https://developer.mozilla.org/en-US/docs/Mozilla/Developer_guide/Introduction
[25] https://opentechstrategies.com/
[26] https://blog.mozilla.org/wp-content/uploads/2018/05/MZOTS_OS_Archetypes_report_ext_scr.pdf

Quick-Reference Comparison Of All Archetypes

	B2B	Multi-Vendor Infra	Rocket Ship to Mars	Controlled Ecosystem	Wide Open	Mass Market	Specialty Library	Trusted Vendor	Upstream Dependency
Main benefit	Driving industry adoption of your technology	Collaboration with partners; address a set of shared problems	Quick, focused effect in a specific area	Can build a sustainable ecosystem in which founding organization has strong influence	Large-scale collaboration; community can become self-sustaining	Large user base can make project broadly influential	Ensure quality solution to a specific problem; can lead to new partners	Loyalty of downstream consumers helps project stability	Broad reach across (hence insight into) many dependee projects
Main drawback	Little or no collaborative development	Sometimes off-putting to individual contributors	Collaboration only available from those who share a very specific vision	Compromise needed to avoid forks (esp commercial)	Effort to maintain onboarding paths & manage all participants	Huge user base needs filtering for dev community	High barriers to entry; relatively small developer pool	Primary org must be careful how it uses its position	Developer base can sometimes be lightly motivated
Main situational consideration	Requires major market power to be effective	Business needs of participants affect community management	Everything depends on success of original vision	Participants have many motivations (commercial & non-commercial)	Differing commitment & engagement levels among participants	Contributor base does not accurately represent user base	Standard-setting effects (de facto or official)	Customer needs vs open source project needs	Usage patterns of downstream consumers
Development speed	Fast; pace set by business goals	Usually moderate, but depends on needs of participants	Fast; escape velocity	Medium	Slow medium; some process overhead	Slow medium; swift change destabilizes user base	Gets slower over time, as library stabilizes	Medium: primary vendor momentum vs third-party needs	Medium; may slow down as standard settles
Component coupling	Tightly coupled, to market one unified product	Loosely-coupled with de facto standards	Tight, to ship one core product	Loosely coupled, often with plugin system	Variable	Variable	Tightly coupled	Tightly coupled	Standalone; decoupled from one another & from downstream projects
Typical participant type	Organizational reps	Organizational reps	Founding organization	Founder, some external core contributors, many plugin contributors	Open to anyone; participant demographic depends on project	Organizational reps, redistributor reps; some users who are technical	Developers with expertise in the relevant field	Customer reps (both paying and non-paying); some one-off contributors	Downstream devs
Typical licensing	Almost always non-copyleft	Usually non-copyleft, because many internal forks	Usually non-copyleft, but with occasional exceptions	Any, but requires thought re plugins	Any	Usually non-copyleft, but depends on business strategy	Usually non-copyleft	Either; copyleft sometimes used to discourage competitive forks	Usually non-copyleft
Ease of onboarding	Hard	Medium	Hard	Medium	Easy	Easy to medium	Depends on technical complexity	Medium to hard	Depends on technical complexity
Community standards	Oriented toward organizations	Welcoming but formal; difficult for individuals	Focused on core group	Welcoming, with some onboarding structures	Very welcoming, formalized onboarding systems	Fully open; scales via users helping users	High barrier; contributors need to be experts	Clear boundaries: users have mainly roadmap input	Welcoming; amenable to one-time contributions
Typical governance	Lead company plus partners	Committee of organizational reps	Founder governs with iron fist	Benevolent dictatorship; tries to avoid forks	Group-based; consensus / democratic	Main organization leads, with outside input	Multi-party committer group	Main vendor leads	Informal, maintainer-led, committer groups
Measures of open source success	1. Adoption by target partners (aiming for dominant levels) 2. Code contributions from partner organizations 3. Successful projects built around core project	1. Partners contributing at equal and high levels 2. Longevity of contribution by committers 3. Variety of organizations contributing	1. Speed of development 2. Adoption by target users 3. Achieving original technical goals	1. Adoption by target users 2. Increase in number of extension developers 3. Overall cohesiveness of community	1. Growth in number of contributors 2. Efficiency of contribution 3. Variety in where decisions get made	1. Awareness among users that project is open source 2. Growth in non-technical contributors 3. Effective filtering of user feedback to developers	1. Adoption by intended domain (perhaps even dominant adoption) 2. High quality of contributors 3. High quality of code	1. Absence of competitive forks 2. Business needs of vendor served 3. Vendor's leadership accepted by community	1. Multiple competitive distributions 2. Longevity of participation 3. Bug reports tend to be technical and constructive
Examples	Android; Chromium	Kubernetes; Open Stack	Meteor; Signal	WordPress; Drupal	Rust (present day); Apache HTTPD	Firefox; MediaWiki (due to Wikipedia instance)	libssl; libmp4	MongoDB; Hypothes is; Coral	OpenSSL; WebKit; just about every small JavaScript library on GitHub

Mozilla Corporation
331 East Evelyn Avenue
Mountain View, CA 94041

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?**

   It is vital that consent, agency, transparency, accessibility, and inclusion anchor the pursuit of improving user engagement. This is the only real way to avoid falling into the pitfalls of the modern surveillance economy.[27] For example, it will be useful to evaluate how many user studies were conducted to evaluate the need for the NODE projects that have already been launched and how the outcomes of these studies were used to shape these projects themselves. Our Open Archetypes report[28] may also be helpful in this regard.

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.**

    In addition to our response to Question 5, the Business and Human Rights Centre's guidance on Non-judicial grievance mechanisms,[29] are a useful source on how to set up grievance redressal mechanisms, both within traditional government frameworks as well as one's that run exclusively within organizations. The exploratory analysis by the University of Manchester for the UN on non-state based non-judicial grievance mechanisms is also a good source for best practices that are followed around the world.[30]

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) ……...**

    While this question can be better answered by other stakeholders who want to build a NODE, Mozilla does have the Common Voice project that could be useful to other NODE projects, as described below.

    Common Voice[31] is a crowdsourcing platform started by Mozilla to create a free database for speech recognition datasets. Providing people with information in their language can be a

[27] https://www.ft.com/content/7fafec06-1ea2-11e9-b126-46fc3ad87c65
[28] See Footnote 27
[29] https://www.ohchr.org/Documents/Issues/Business/ARP/ManchesterStudy.pdfhttps://www.business-humanrights.org/en/un-guiding-principles/implementation-tools-examples/access-to-remedies-grievance-mechanisms/non-judicial-grievance-mechanisms
[30] https://www.ohchr.org/Documents/Issues/Business/ARP/ManchesterStudy.pdf
[31] https://voice.mozilla.org/en

key driver of economic empowerment and political participation. However, the diversity and lack of technological support for spoken languages in India makes universal access to information and services an ongoing challenge. Artificial intelligence (AI) and machine learning (ML) offer novel and efficient ways to tackle this challenge. AI-based voice recognition has great potential to make technology more inclusive and enable millions of people to access services they are not able to use yet – be it in agriculture, education, health, or other sectors.

The lack of free and open voice data to develop and train language processing models is a fundamental barrier to achieving these outcomes. Although many ML algorithms are in the public domain, training data is not: Most of the voice data used by large corporations is not available to the majority of people, expensive to obtain, or simply non-existent for many languages. For example, the most widely used voice assistant in the country (Google Assistant) is only available in 9 languages, despite India having over 22 languages recognized by the constitution. The innovative potential of this technology is widely untapped. With providing open datasets, Mozilla hopes to take away the onerous tasks of collecting and annotating data. It reduces the main barriers to voice-based technologies and creates a potential market for tech innovators and social entrepreneurs. While Common Voice is not a NODE-like project, it could solve many of the challenges of user engagement faced by other projects under the Strategy.

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

    As mentioned in our opening letter, the 'Mozilla and the Rebel Alliance' report[32] might be a helpful tool in studying how Mozilla manages open source project networks and communities. Some other useful resources on this front would be Mozilla's Open Innovation Wiki[33] and Blog[34] along with our new Community portal.[35]

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?**

    All outreach and capacity building under a NODE project (independent of its tools) should be transparent, accountable, and inclusive. We recommend that MeitY hold at least one more

[32] See above
[33] https://wiki.mozilla.org/Innovation
[34] https://medium.com/mozilla-open-innovation
[35] https://community.mozilla.org/

generic public consultation with an improved white paper that addresses the concerns expressed by various stakeholders. For example, this could include providing more visibility into how the NODE model will interface with existing laws and regulations. As a part of that consultation, regular workshops with diverse stakeholders should be held to aid multi stakeholder inputs, including civil society groups outside the technology sector. This will enable different stakeholders to be able to know when they can contribute to a process and how they can be effective in having tangible impact.

Once the strategy itself is implemented, specific public consultations on NODE projects, along with the institutionalization of public bug bounty and security audit reports, will go a long way in ensuring that the high-level principles of this strategy are implemented effectively. Critical to enabling these models is adopting multi-stakeholder governance, which as articulated in the 2005 Tunis Agenda for the Information Society,[36] recognizes the importance of involving all stakeholders in governance, including government, the private sector, the technical community, and civil society.

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

Mozilla will be happy to share its learnings in managing some of the most widely used open source projects in the world in either individual consultations or as a part of public workshops. We will also be happy to explore how Common Voice, a crowdsourcing project started by Mozilla to create a free database for speech recognition datasets, can be leveraged to aid NODE projects by making them accessible in a wider variety of languages.

[36] https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html