Mozilla Corporation
331 East Evelyn Avenue
Mountain View, CA 94041

To

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

31 January 2021

We thank the Ministry of Electronics and Information Technology (MeitY) for the opportunity to provide feedback on the second iteration of the Report by the Committee of Experts on Non-Personal Data Governance Framework (hereafter, "the report" or "report"). We welcome the move to have a second round of consultations on an iteratively improved report 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 highlights, there are over 22,000 contributors in over 49 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 also in our policies and in the open source code of our products.

We appreciate the various improvements made in the second version of the report, specifically those that move away from mandatory data sharing between private entities, the creation of distinct frameworks for both personal and non-personal data and most importantly the explicit introduction of protections regarding the misuse of NPD. These changes showcase that the Committee meaningfully considered the diverse range of feedback during the first public consultation and has set a strong precedence for similar consultations in the future.

However, we would like to bring to your attention that certain key components of the report still containing a worrying spate of measures that would harm Indians, isolate Indian companies from their global counterparts, and cause other countries to retaliate with similar "data nationalisation" measures that would be counterproductive to India' interests. While concerns around the mandatory sharing of such data with private companies has been mitigated to some extent, the focus on governments being able to demand access to such data without sufficient oversight and accountability is still a present in the new report. Keeping this in mind, we would like to reiterate some of the salient aspects of our earlier submission and request that they be considered in the final version of the report:

Mozilla Corporation
331 East Evelyn Avenue
Mountain View, CA 94041

- **Treating data as a national resource undermines individual autonomy -** The Report, in different stages, states that the data of Indians is a "national resource" and that rights surrounding it should be governed similar to "economic rights over natural resources." This framing, founded on a flawed model of data ownership, undermines the Supreme Court of India's decision in Puttaswamy v Union of India as well as India's commitments under the International Covenant on Civil and Political Rights. The Puttaswamy judgment held in no uncertain terms that the fundamental right to privacy was "an intrinsic part of the right to life and liberty", predicated on the dignity and autonomy of every individual. To replace this fundamental right with a notion of ownership akin to property, vested in the individual but easily divested by state and non-state actors, leaves individual autonomy in a precarious position.
- **Forced data transfers are not a solution to the concentration of market power -** Non-personal data can constitute protected trade secrets and the insights derived from such data may be protected by intellectual property law, both of which would raise significant concerns around the fundamental right to carry out business and India's obligations under international trade law. Turning over this information to the government without any checks and balances also raises significant privacy concerns. Information about sales location data from e-commerce platforms, for example, can be used to draw dangerous inferences and patterns regarding caste, religion, and sexuality. Therefore, we recommend that the "Sovereign" purpose exemption in the new report be better defined and contain a clear list of criteria that meet the standard of necessity and proportionality prior to its invocation to protect the fundamental right to privacy.
- **Re-identification poses grievous risk to privacy and security -** The report also notes the value of "anonymized and aggregated data" towards creating "data trusts". We acknowledge and support the release of more open datasets that might spur innovation in India. However, we would also warn that research has consistently shown that there are serious risks of re-identification even with apparently anonymized datasets. Paul Ohm's seminal paper concluded that "Data can be either useful or perfectly anonymous but never both." A study by Latanya Sweeney found that 87.1% of people in the United States were uniquely identified by their combined five-digit ZIP code, birthdate, and sex. Another study re-identified data subjects based purely on their movie preferences on Netflix. In light of these risks, we would urge the government not to make the blanket assumption that the public release of datasets is an acceptable risk.
- **Consent for Non-Personal Data -** Anonymization is a privacy respecting technique and custodians should be permitted to anonymize data without the need for obtaining any additional consent. The report states that "Personal Data that is anonymized should continue to be treated as the Non-Personal

Data of the data principal." This is inherently contradictory, as anonymisation should make it infeasible to be able to distinguish between one data principal and the other. Such a move may force data custodians to not anonymise data sufficiently to be able to track such consent, placing such data at an additional privacy and security risk. Alternatively, it would require the re-identification of the principal in an anonymized dataset. Doing either of these things would defeat the whole purpose of the anonymization in the first place. Further, the requirement that data collectors should separately provide notice and offer the data principal the option to opt out of data anonymisation is also worrying both from an innovation and protection of privacy perspective. This ambiguity should be clarified to prevent data subjects from being harmed due to unclear legislative drafting.

- **Community data is a nebulous idea and needs clarity -** The definition present in the report continues to be incredibly wide ranging and is ill suited to a framework that is being designed to enforce rights and protect the interests of its constituents. Under this classification, religious groups; people from the same educational institutions; vulnerable communities based on class, caste, and economic criteria; and people who once lived in a residential locality, are all valid communities with enforceable data rights. They can all have conflicting interests over data that they may have shared with government and private platforms. For example, a housing society that wants to raze neighbouring trees to build a new road and an opposing group of environmental activists from the same society could ask for both aggregate tree cover data from a mapping provider. With overlapping members, the report doesn't provide the criteria by which the mapping provider should choose between them as the representative 'community' to respond to in this case. Without a guiding legal framework or principles, which is absent in the report, such a model will have a crippling effect on service providers from a compliance perspective. They will be forced to make legally binding decisions on what is a valid community, what is the scope of data that can or cannot be shared with such communities, and how to resolve disputes between competing claims to represent a community's interest. The scope of exclusion and discrimiation, which many communities already suffer from, will only increase with such a model.
- **Data trusts need to be explored more rigorously -** The report defers most questions on how data subjects and data custodians will interface with each other via data trusts and data trustees. While it talks about the need for a regulatory framework for such entities, it doesn't lay out any detailed criteria for how they would operate in practice. Mozilla is currently looking into different types of data governance models, such as trusts, as we believe this concept may hold promise. However, there are a range of challenges and complexities associated with the concept that will require careful navigation in order for trusts to meaningfully improve the state of data management and to achieve a truly ethical and trustworthy data ecosystem. Similarly, the new idea of "High Value Data Sets (HVD)" in the second

Mozilla Corporation
331 East Evelyn Avenue
Mountain View, CA 94041

draft also requires better clarity on the mechanisms for protecting privacy, security and the constitutionally guaranteed fundamental rights before it is recommended for implementation. We believe that the report should explicitly call this out and focus on these models being studied rigorously prior to them being implemented in any form.

We recommend that the government reconsider the idea of creating a non-personal data governance framework at this time and focus on implementing an effective data protection framework instead. Once India has an effective data protection law, the process for creating a non-personal data regulation should be started afresh with much greater input from civil society and impacted communities.

Warm regards,

Udbhav Tiwari
Public Policy Advisor