January 31, 2021

To
Shri Ajay Prakash Sawhney
Secretary (Electronics & Information Technology),
Union Ministry of Electronics and Information Technology,
Government of India,
New Delhi.

Subject: Access Now's submission to the call for comments on the Revised Draft Non-Personal Data Governance Framework

We write to you in connection with the call for comments from the Ministry of Electronics and Information Technology (Meity) regarding the revised report of the Committee of Experts on Non-Personal Data Governance Framework (NPD Report). We had also provided our comments to the initial call for comments on the first draft of this report.

Access Now is an international non-profit organisation which works to defend and extend the digital rights of users at risk globally. Through presence in 13 countries around the world, Access Now provides thought leadership and policy recommendations to the public and private sectors to ensure the internet's continued openness and the protection of fundamental rights. Access Now also engages with its global community of nearly half a million users from over 185 countries, in addition to operating a 24/7 digital security helpline that provides real-time, direct technical assistance to users around the world. We coordinate as part of CiviCERT (Computer Incident Response Center for Civil Society) a Trusted Introducer accredited CERT. We also have special consultative status at the United Nations.[1]

At the outset, we would like to thank the Ministry for inviting comments as part of its consultation on the committee's revised report. The revised report shows that the committee is responding to several of the concerns flagged by stakeholders to the first draft report. Our comments below go into our detailed suggestions on our top level concerns. At the overall level, we strongly recommend that the committee and the Ministry recognise that this proposed non-personal data

[1] Access Now, *About us*, https://www.accessnow.org/about-us/.

governance framework is premature to advance as a legislative priority at this time, and would raise significant issues that would impair the enactment, enforcement, and institutionalisation of data protection measures in India. The creation, advancement, and actual implementation of a data protection framework that secures the data protection rights of Indians and better secures their fundamental right to privacy must be the overriding objective. We therefore believe that the outcome of the work of the committee of experts on non-personal data governance framework should be a set of recommendations and their rationale which is designed to be then studied by the Data Protection Authority set up by the Personal Data Protection law once passed. A standalone law on non-personal data before the Data Protection Act comes into force and is meaningfully enforced would be premature and harmful to protecting privacy and ensuring effective data protection governance. Protecting individuals and vulnerable communities requires data protection rights and their enforcement to be clear.

In addition to this top level concern, our more specific inputs to the revised report are the following:

1. **Restrict and minimise use of data from users; do not treat the exploitation of their data as the main policy goal**
2. **Data protection law and its regulatory enforcement should be the top policy priority**
3. **Problematic legal structure of proposed non-personal data framework and its standalone regulator**
4. **Treatment of Anonymised Data as Non-Personal Data**
5. **High Value Datasets and the Role of Data Trustees**
6. **Overbroad data sharing for "sovereign purpose"**
7. **Creation of a regulatory vacuum in relation to sharing of anonymised data for business purposes**

Below we provide our substantive comments on the NPD Report and framework below. Kindly note that our comments in response to the initial report still stand, if not clearly amended in this version of the comments. We have not replicated all comments in this version, for the sake of brevity.

1. **Restrict and minimise use of data from users; do not treat the exploitation of their data as the main policy goal**

We continue to be concerned that the Committee of Experts - as seen in this revised report - is advocating for a framework that sees its main basis in extracting value from data originating from users. Any policy or legal framework on data - whether provided by, originating, related to, or inferred from a person - must keep the person and their rights in the front and center of the

policy. Indeed, as we noted in our filing on the initial draft report, this this argument has found credence in the seminal judgement of *Justice K.S.Puttaswamy(Retd) vs Union Of India,* which clarified the position of the right to privacy as a fundamental right, guaranteed by the Constitution of India.

Data minimisation and purpose limitation should be the core pillars of any legal framework concerning data. The revised non-personal data report continues to suggest an approach wherein entities must collect a lot of data; this data must be shared with other companies and entities using data exchanges; and used to "innovate" solutions for India. We again reiterate that this "collect now, use later" approach to data governance must be avoided, and the pillars of purpose limitation and data minimisation must be promoted. Data governance frameworks should focus on protecting the rights of users, and putting them in control, rather than establishing the ownership of data with companies.

While we applaud the effort to restrict the applicability of the framework to data sharing requests to "public good" needs - instead of the other purposes mentioned in the initial report such as those of business and security - the principle objection regarding the vagueness of the standard of "public good" and the lack of clarity regarding the need for such a framework remain, especially with the lack of a data protection framework in the first place.

2. **Data protection law and its regulatory enforcement should be the top policy priority**

There is an urgent need at present in India to regulate personal data and provide rights and remedies to users. As we have stated previously, It is only after the development of a fairly mature data protection framework in India that a framework for non-personal data should be established. A privacy and data protection framework would provide the contours of the rights of users, which is of primary importance. Once such contours and remedies for breaching these contours are developed, the Data Protection Authority can work with MEITy in establishing a governance framework for non-personal data. Creating a standalone regulator for non-personal data would divide critical government focus, place competing claims on scarce public resources, increase institutional conflict and regulatory confusion, consequently harming the protection of privacy and jeopardizing the public interest. Establishing a framework for non-personal data before the contours of rights for personal data are developed would inhibit the working of the Data Protection Authority. Only once a comprehensive law is enacted, and a truly independent and strong regulator is put in place, would India be able to move towards properly governing the use of non-personal data and develop specific regulations and best practices.

The revised report has aggravated this problem further. The revised version of the report imagines a non-personal data framework which is exclusive from the privacy and data protection framework. This imagination would create constant conflicts between the jurisdictions of the proposed data protection authority and the authority which would regulate non-personal data. With the lack of a jurisdiction of the proposed data protection authority, over non-personal

data, it would not be able to protect the rights of individuals in cases where the contours between personal and non-personal data are not clear. In fact, this essential determination should be made by an independent data protection authority, with constant continuing supervision exercised by the authority.

3. Problematic legal structure of proposed non-personal data framework and its standalone regulator

In addition to the recommendation we make in the section above about the need to prioritise the personal data protection framework, we also see concerns from the legal approach proposed in the revised report and the initial outline of the proposed non-personal data authority (NPDA). The revised report is unclear in its constitutional rationale for why a non-personal data governance framework should be passed as a central law by the Parliament of India in India's federal system. Several of the illustrations in the revised report give examples of data whose collection or proposed use relates to matters falling under the state government or local government. The definition of non-personal data in the revised report does not appear limited merely to matters relating to communications - which falls under the Union List in the Constitution of India - but to a broader category pertaining to all digital information and database creation. It would be crucial at the very least for the Committee of Experts and MEITy to clarify this issue and provide their understanding of the legal authority and rationale for a union-level legislative framework on this issue. Consultations should also take place with the state governments and local government authorities.

In addition to federal issues, the revised report has outlined a vision of a non-personal data authority which in itself raises issues. The revised report contains scant details on what exact form the authority would be established; who would constitute its membership, how would it be staffed, how would appointments be made to the authority, what relationship would the Union Government and state governments have with it? The revised report speaks to the need for harmonisation with the Data Protection Authority and Competition Commission of India, but at present does not suggest how this would take place. Given the many instances of how regulatory overlap already causes issues between existing bodies such as the CCI and TRAI - despite the existence of specific legal provisions on consultations amongst regulators - it is crucial that the Committee of Experts provides more detail on its proposed approach on regulatory design. The issue of regulatory design is also crucial given that regulatory independence is even more crucial in this context, where a range of government agencies are envisaged as playing potential roles of data trustees, data requesters.

The one clear recommendation that the revised report does make is that the NPDA "must be created with industry participation". This emphasis on embedding only one type of stakeholder - industry - with the creation of the NPDA is alarming. This gravely undermines statements elsewhere in the revised report on the focus of the non-personal data framework being

ostensibly towards safeguarding communities and advancing public interest concerns. There appears to be no prioritisation of involvement of other stakeholders in the establishment, design, and operation of the NPDA.

Additionally, the revised report proposes several "enforcing function" elements of the NPDA which appear to directly conflict with the DPA under the Personal Data Protection law. The function to "address privacy, re-identification of anonymised personal data, prevent misuse of data" would be a primary role of the DPA; this should not be carried forward in the final recommendations of the Committee of Experts.

4. Treatment of Anonymised Data as Non-Personal Data

The revised report suggests that in order to extricate non-personal data from the ambit of a future personal data protection framework, certain clauses in the proposed PDP Bill 2019 must be removed to extricate "anonymised data" from this bill. This must not be done. As the report recognizes, anonymised data in many instances has been re-identified, either due to the availability of new technology or the lack of sophistication or negligence on the part of the anonymising entity. It is ironic that while the report recognizes that anonymised data is susceptible to re-identification and therefore, causing privacy harms to people, the report suggests that such data must be put outside the ambit of the privacy protection framework and authority.

Further, while the report seems to suggest that data once re-identified would fall within the ambit of the data protection authority, it does not provide any clarity on how privacy harms would be adjudicated upon, resolved and undone in case freely shared anonymised data under the non-personal data framework becomes re-identified. One can only imagine a regulatory response which mimics the adage - no point crying over spilt milk.

At its core, anonymised data is personal data and should not be governed solely by the NPD framework and proposed NPDA. Existing research has found that in many instances anonymised data can be very easily used to re-identify individuals. As an example, researchers published a method in 2019 that "is able to correctly re-identify 99.98% of individuals in anonymized data sets with just 15 demographic attributes".[2] Further, the methods of de-identification or anonymisation are required to be as per protocols developed by the Government of India. The pace of the movement of technology and its use for re-identification would be too high for hard coded regulations to be able to keep them in check over time.

---

[2] *Researchers spotlight the lie of 'anonymous' data*, 2019. https://techcrunch.com/2019/07/24/researchers-spotlight-the-lie-of-anonymous-data/ ; citing Rocher, L., Hendrickx, J.M. & de Montjoye, YA. *Estimating the success of re-identifications in incomplete datasets using generative models*, Nat Commun 10, 3069 (2019). https://doi.org/10.1038/s41467-019-10933-3.

The revised report takes away the already inadequate requirement of consent of the data principal for anonymisation and the sharing of anonymised data. The revised report instead only provides that an opt-out from anonymisation would be provided to users. A user who is sharing their data for a specific purpose with an entity should be assumed to consent that their data may be anonymised and shared with any entity for the "public good". There is no basis for this assumption provided in the revised report. If in fact this framework is to be further advanced, it should require clear consent for anonymisation and further use by requiring that the originating individuals explicitly opt-in to further use of their data after anonymisation.

5. High Value Datasets and the Role of Data Trustees

The initial NPD framework seeks to establish a new class of data called community data. As per the framework Community Non-Personal Data *"means Non-Personal Data, including anonymised personal data, and non-personal data about inanimate and animate things or phenomena – whether natural, social or artefactual, whose source or subject pertains to a community of natural persons".* Whereas Community is defined as "*any group of people that are bound by common interests and purposes, and involved in social and/or economic interactions. It could be a geographic community, a community by life, livelihood, economic interactions or other social interests and objectives, and/or an entirely virtual community".* In essence, non-personal data belonging to users is an oxymoron. Data about communities which may be seen to be bound by common interests such as social or economic interests is being called community data.

This is a very vague definition and has huge implications on the data governance framework for non-personal data. The revised report provides some element of clarity wherein data custodians have been defined as entities which collect, store and process user data. They are also responsible for anonymising data. A new addition through the revised report is "High Value Datasets". These HVDs seem to be datasets which benefit a community at large and would be maintained by data trustees. Data trustees would be governmental or non-profit organisations who would be responsible for creating and maintaining HVDs.

The definition and standard for HVDs are vague and subject to interpretational issues. Data requests for maintaining or creating HVDs must be accepted by data custodians. Data trustees would make these requests. The structure of Data Trustees and the obligatory nature of data sharing would promote a high data sharing environment which would make data susceptible to huge harms to people on re-identification. It still remains unclear how data trustees will be able to clearly demonstrate they are a legitimate representative of the community they claim to act on behalf of. In such an uncertain regulatory environment, there is an increasing risk of non-representative agencies establishing themselves as data trustees and becoming the gatekeepers on the rights of users. Personal data and the accompanying rights must be housed in the individual and alienation of these rights to other agencies should be avoided, especially when such agencies are so vaguely defined. While innovation is welcome, it is important to note

that such structures do not exist in any regulatory jurisdiction - even those with much more developed data governance frameworks than ours.

6. Overbroad data sharing for "sovereign purpose"

The revised report indicates that the Committee of Experts has identified "Sovereign Purpose" as one of the three purposes for non-personal data sharing. At present, the revised report provides insufficient clarity on what would constitute such sovereign purposes and their corresponding legality. It lists possible cases which are tremendously broad - all sorts of security vulnerability mapping and response, law enforcement agency initiatives - including anticipatory measures, and pandemic mapping are listed as illustrations. The revised report states that "already regulations exist in India which address sharing of data for Sovereign purpose" but provides no references or authority to back this claim and what the Committee of Experts believes are currently authorised sovereign purposes. The Justice Srikrishna Expert Committee on Data Protection in fact noted an contrasting finding; indicating that many elements of Indian data access powers by law enforcement and security services were not clear in their legal authority and in fact may conflict with the raised standards around the fundamental right to privacy as articulated in the Puttawamy 9-judge bench ruling of the Supreme Court. The proposed non-personal data governance framework must explicitly list all the legitimate sovereign purpose cases it proposes to include and further explain what oversight and checks on such state powers will be included. The revised report merely says that the PDA will not adjudicate the validity of data requests in the case of sovereign purpose, leading us to ask the question: who then would do so?

7. Creation of a regulatory vacuum in relation to sharing of anonymised data for business purposes

The revised report excludes "business purpose" from the ambit of the non-data protection framework, and more worryingly, excludes anonymised data from the ambit of the proposed data protection regulation. These two exclusions have created a regulatory vacuum when it comes to the sharing of anonymised data from business purposes. As has been noted by the report itself, anonymised data has inherent reidentification risk with huge consequences for users. Anonymised data must be regulated by the proposed data protection authority. Under the current proposal, it seems that sharing of anonymised data between businesses would be unregulated - putting in huge risk for users.

Conclusion

As mentioned in our initial submission, the regulatory domain of non-personal data in India should be built on the right to privacy and be framed in a human rights focused approach. It is our recommendation that India must pause and reflect on its non-personal data governance

framework, establish open and transparent consultations and only seek to establish a limited framework after the passage and implementation of a comprehensive data protection and privacy framework in India, along with adequate surveillance law reforms. The immediate task at hand is to establish this data protection and privacy framework and protect the rights of users' personal data. Exploratory work into the area of non-personal data should not come at the cost of this pre-existing priority.

We remain at your disposal to respond to any queries or provide any other assistance.

Sincerely,

Naman M. Aggarwal
Asia Pacific Policy Counsel and Global Digital Identity Lead
naman@accessnow.org

Raman Jit Singh Chima
Asia Pacific Policy Director and Senior International Counsel
raman@accessnow.org