September 13, 2020

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 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 report of the Committee of Experts on Non-Personal Data Governance Framework (NPD Report). We write to you to provide our comments based on our expertise working on data protection laws and related issues of technology policy across the world, including India.

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 initial report, and we appreciate the opportunity to provide inputs and we hope that these will be helpful to the Ministry in thinking through the NPD Report and the proposed framework. We also appreciate the extension of the original one week deadline for comments by the Ministry, after repeated calls from civil society and other stakeholders. Open, transparent and comprehensive consultations are an essential backbone of policy making in democracies. We shall be making our submission to the consultation public, and urge the Ministry to make all submissions public, in line with the practices followed by other regulators and government agencies in India and the global standard expected in this area.

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

Below we provide our substantive comments on the NPD Report and framework:

1. **Data belongs to the user, not the company**

The NPD Report and framework finds its basis in extracting value from data for enterprises, primarily those based in India. While there are mentions of privacy and data protection, the prime focus remains on leveraging data for the benefit of economic value creation. At the outset, we would like to state that personal data belongs to the user, and not the entity (the "data fiduciary") which collects, stores or uses this data from the former (the "data principal" or user). Any policy on personal data - 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.

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. Even the Personal Data Protection Bill 2019 - currently under consideration before Parliament - presupposes the primary right of users over their data, and the role of entities collecting data as a fiduciary in relation to the data of the user.

Two of the pillars of a strong and comprehensive privacy and data protection regime are the principles of purpose limitation and data minimisation. Purpose limitation provides that the data collected by a fiduciary of an individual must only be used for narrow and defined purposes. Data minimisation provides that the processing, including collection and retention, of data of the user by fiduciaries must be minimised and limited to data which is necessary in relation to the identified purpose. By contrast, the proposed non-personal data framework provides a syntax wherein companies must collect a lot of data, this data must be shared with other companies using data exchanges, and used to innovate solutions for India. It shall be noted that "innovation" in itself is not a specific purpose and more specific goals must be identified to comply with the principle of purpose limitation. Using such a syntax for data governance in India will prompt companies to collect excessive data and later figure out possible uses for it. 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.

2. **Urgent need for a data protection law and regulator**

India, the largest democracy in the world and second-largest internet user base, has been trying to enact a national data protection law for quite some time now. The Personal Data Protection Bill, 2019 (PDP Bill) which has been approved by the Union Cabinet and was placed in the Lok Sabha is currently under review to a Joint Parliamentary Committee - consisting of members of both houses. The Joint Parliamentary Committee's process has been delayed and handicapped due to the non-functioning of much of the Indian Parliament during the COVID - 19 pandemic.

The vision of the NPD Report at its centre is to regulate non-personal data. It seems chronologically counterproductive to regulate non-personal data before regulating personal data, which implies defining its scope. There is an urgent need to regulate personal data and provide rights and remedies to users. 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.

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.

3. Defining Non-personal data and its sharing

The NPD Report provides that two kinds of data were considered under the framework -
1. Data that never related to any identifiable or natural person;
2. Data which were initially personal data, but were later made anonymous.

It is very important that these kinds of data be governed and regulated separately, as they have a very different ambit and impact on users.

We welcome the decision to regulate non-personal data which is not related to any identifiable or natural person, especially data which is collected and stored by the Government of India. The Government of India should build on previous open government and open data focused policies such as the National Data Sharing and Accessibility Policy (NDSAP 2012), and promote the disclosure of information held by government departments in a proactive and transparent manner. However, the situation related to anonymised data, which are in fact personal data, is very different and far more complicated.

The NPD Report provides that anonymised data held by data fiduciaries, including the government, may be made available to many companies and institutions for various purposes such as sovereign purposes (national security), public interest purposes (statistical analysis, public policy making) and economic interests (leveling the playing field, promoting Indian startups). While the intent of the provision seems to be to promote interests of the Indian ecosystem, the result of the provision may be to open up users to exploitation and drive-away developers from India. At its core, anonymised data is personal data and should not be

governed by the NPD. 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.

The NPD framework states that consent of the data principal would be taken for anonymisation and sharing of anonymised data However, this proposed safeguards is likely to be insufficient and cannot be properly actionable in a context where India does not have a data protection law and authorities. In fact, users would be left without remedy or actionable rights in case of abuses. Given their nature as personal data, as recognised by this report when suggesting seeking users consent, the use and governance of anonymised data should be dealt with in the PDP law, not the NPD policy framework.

4. Purposes for collection and sharing of non-personal data

It is important to note that the Government of India is perhaps the largest collector of data in India. The Srikrishna Committee report, which was the originator of the draft Personal Data Protection Bill, has stated the need for surveillance reform in India and pointed out that adequate checks and balances do not exist in India when it comes to government access to personal information. The Indian Supreme Court has also laid down that Indian law follows the international best standards of principles of necessity and proportionality for governmental access to data.[3]

Specifically, the standards of sovereign purposes, public interest purposes and economic purposes must provide adequate safeguards required to ensure that the lawful access of information by government agencies holds up to the standards of necessity and proportionality,[4] reiterated by the Supreme Court of India is the seminal judgement of Justice K.S. Puttaswamy vs Union of India.[5] It has been propounded by the court that infringement to the right to privacy must satisfy the standard of necessity and proportionality. This standard provides the requirement of (i) a "law", (ii) a "legitimate purpose", (iii) the action being "necessary in a democratic society", (iv) the interference to the fundamental right being "proportionate to the need of such interference" and (v) "procedural guarantees against abuse".

---

[2] Researchers spotlight the lie of 'anonymous' data, 2019. https://techcrunch.com/2019/07/24/researchers-spotlight-the-lie-of-anonymous-data/?guccounter=1

[3] https://www.eff.org/files/necessaryandproportionatefinal.pdf

[4] Available at https://necessaryandproportionate.org/principles

[5] Available at https://www.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf

The draft framework provides a very vague and broad action matrix of sharing non-personal data such as sovereign purposes, public interest purposes and economic purposes. Evaluation of this matrix on the threshold of necessity and proportionality proves to be an unachievable task. It is important that the action matrix be limited, as the Supreme Court judgement in the right to privacy provides that the burden of proof of necessity and proportionality lies on the government.

Further, the non-personal data framework provides preferential access to “Indian startups” in relation to non-personal data collected from big technology companies. While we appreciate the sentiment of regulating the dominance of big technology companies and promoting startups in India, we must warn against the subjugation of rights of users for these purposes and the development of a “collect all data” ecosystem. For example, even seemingly “startup” organisations can choose to undertake harmful, privacy-impacting practices - as seen in the business decisions and conduct of firms such as Cambridge Analytics, Clearview AI, and many others. It has been time and again also shown that massive collection of data is not only harmful for users but also legitimate data businesses in the startup ecosystem.

5. Community Data and Data Custodian

The 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. Under this framework, data custodians shall act as representatives of communities, when it comes to requests for sharing and collection of data. These structures have not been defined and it is very difficult to establish representatives of the vaguely defined communities. In such an uncertain regulatory environment, there is an increasing risk of non-representative agencies establishing themselves as data custodians and becoming the gatekeepers of 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. The governance of these data shall therefore also be discussed within the PDP Bill.

6. Reliance on the European Union frameworks on movement of non-personal data

The NPD Report seeks to rely on the example of the European Union policy for free flow of personal data.[6] It is important to understand that after adopting a comprehensive and upgraded data protection law and legislation on the free flow of data, an European data strategy is currently under consultation and is being developed further. The current policy is only limited to the free flow of non-personal data (i.e. data which does not relate to any identifiable or natural person) and does not include anonymised data but defining this scope was only possible once the framework on protecting personal data was completed. The policy in the European Union also does not currently promote excessive collection of data or the sharing of non-personal data between companies - this policy is only in relation to storage of data within the ambit of the same enterprise. Lastly, and perhaps most importantly, the European Union is home to the General Data Protection Regulation which provides the users in Europe rights in relation to their data. It is only after the development of a mature data protection framework that the European Union has embarked on regulating non-personal data - only to the limited extent of storage of such data, and not sharing of such data on grounds such as sovereign purpose, public interest purpose and economic purpose. India would do well to learn from the example in the European Union - while listening to its own community and stakeholders outlining the importance of taking steps to advance a clear focus on strengthening the right to privacy and other fundamental rights in this digital age.

Conclusion

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.

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

Sincerely,

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

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

[6] https://ec.europa.eu/digital-single-market/en/news/free-flow-non-personal-data