#NAMA: Recommendations for governing non-personal data; what data trusts are

The government should draw inspiration from the Personal Data Protection Bill, 2018, to oversee government access to non-personal data, and there must be a system of checks and balances, a speaker said at MediaNama's roundtable discussion on non-personal data, held in November 2019. A number of recommendations for governing non-personal data emerged. Most participants agreed that any framework that the government or the committee of experts on non-personal data came up with should keep the following questions in mind:

- What is the due process of law?
- Who orders access to non-personal data? Is it responsible enough?
- What are the checks and balances in place for this access?
- Does it pass the test of public good?
- Where should those checks and balances be in place across the industry?
- When can the government make a trade-off between group privacy/autonomy and social good? Proportionality analysis of harms is necessary to answer this question.

Under this framework, a speaker clarified, the government should actually notify what data sets come under public good, national security, etc., and if they pass those tests. However, a participant disagreed and said that we don't need separate regulation for non-personal data and instead called for a more general protection against misuse of *all* data.

(Note: The discussion was held under the Chatham House Rule; quotes have not been attributed to specific people. Quotes are not verbatim and have been edited for clarity and to preserve anonymity. Also note that this discussion took place before the PDP Bill, 2019, was made public.)

Recommendations on governance

Public interest as a test, but share data with rivals on a case-by-case basis: A speaker said that when the government wants data for public policy, public interest is the obvious test. But for sharing data with competitors, it should be adjudged on a case-by-case basis; the government cannot decide that, it can only decide in terms of public interest.

Consider economic costs of sharing data with rivals: "If companies are chilled by the idea that the data sets they create are now going to be shared with their competitors, there may be an economic cost there that it's not going to be accounted for," said a speaker. The aim is to encourage, not stifle, innovation.

Targeted requests for data sharing to be handled by third-party: A participant suggested that targeted requests for data sharing should be handled by a third party. Also, there have to be clear rules about (mis)use and liability. Completely anonymised data can be put on MeitY's Open Government Data

Platform, and so can data that a private company volunteers to share with everybody.

Database rights are the way forward in the private use context: "Compelling access to a database protected under copyright would be akin to nationalising the data set," argued a participant. And if that is what we are considering, we need to answer questions such as: what sort of eminent domain principle works over here? What are the guard rails? How do you compensate?

Have industry-specific data regulator: Another speaker recommended that data be a part of a regulator for every industry since the "standard of data sharing is very domain-specific". For instance, an insurance regulator should have a department which specialises in data affairs, including its sharing, exchange, publicly available data sets, etc. One speaker said that the Data Protection Authority, proposed in the Personal Data Protection Bill, 2018 (and later in 2019), should not regulate NPD as it has too many things to sort out. Another speaker, agreeing with them, said, "With over 625 million internet connections, more than 500 million internet users, we will need a few DPAs to deal with the kind of issues we have in privacy itself."

The concept of Data Stewards/Trusts/Exchanges

"The data steward sort of sits between the users and entities as well as people who are acquiring the data," a participant explained. A data steward/trust:

- Has a responsibility or duty of care towards the users whose data it is.
- Potentially look at data as labour.
- Helps you negotiate better with technology companies.
- Looks at what the data is being used for.

Data trusts, according to the speaker, could be used to help share data between users and between entities. They could also answer questions such as how do we think about technology standards, quality of data, etc. Another speaker compared it to a regulatory sandbox. A different speaker called it a "good theoretical/conceptual framework to think about federated data governance for non-personal data".

*

Read our coverage of the our discussion on Non-Personal Data in Delhi here. The discussion was held in New Delhi on November 28, 2019, with support from Amazon Web Services, Facebook and FTI Consulting.