Comments on the Report by the Committee of Experts on Non-Personal Data Governance Framework

by

The Bachchao Project

I. Preliminary

This submission presents comments by The Bachchao Project (**"TBP"**) on the Report by the Committee of Experts on Non-Personal Data Governance Framework[1], dated July 12, 2020, released by the Ministry of Electronics and Information Technology (**"the MeitY"**), Government of India (**"the report"**).

TBP commends the MeitY for its efforts at seeking inputs from various stakeholders on this important and timely issue. TBP is thankful for the opportunity to put forth its views.

This submission is divided into three main parts. The *first* part, 'Preliminary', introduces the document; the *second* part, 'About TBP', is an overview of the organization; and, the *third* part, 'Submissions on the issues' contains our comments on the contents of the report.

II. About The Bachchao Project

The Bachchao Project is a techno-feminist collective that undertakes community-centric efforts to develop and support open source technologies and technical frameworks with the goals of mitigating gender-based violence and working towards equal rights for women, LGBTQIA+ people, and gender-diverse people. We conduct research and advocacy in all the above areas and guide communities in determining appropriate technological interventions for themselves.
Website: http://thebachchaoproject.org

This submission has been prepared by Rohini Lakshané, Director (Emerging Research), and Mythri Prabhakara, Volunteer, on behalf of The Bachchao Project on **September 13, 2020.**

---

[1] https://static.mygov.in/rest/s3fs-public/mygov_159453381955063671.pdf Last accessed 13 September 2020.

This submission was submitted at Mygov.in: https://www.mygov.in/task/share-your-inputs-draft-non-personal-data-governance-framework

III. Submission on the issues

1. We submit that the framing of data as an economic resource for commercial activities does not align with the fact that privacy is a fundamental, inalienable right. The language of the non-personal data framework (hereinafter "**the framework**") stands to provide avenues to impingement on rights that are constitutionally and legally guaranteed to citizens. We urge the Committee of Experts on Non-Personal Data Governance Framework (hereinafter "**the Committee**) to be cognizant of the fact that the fundamental right to privacy cannot be waived, even by the holder of that right, even if they agree to write it off.

2. We urge the Committee that the framework use a human rights approach, along with its existing approaches, to analyse both private rights and public rights involved in the context of processing and sharing non-personal data.

3. The existing approach of the framework considers economic gain from viewing data as property for its value generation capacity in the data economy. However, it does not consider a different set of problems, priorities, and solutions to complicated questions about data sovereignty such as:
    - The rights of individuals over their own data.
    - Safeguards to prevent violation of those rights
    - Redress mechanisms in the event that those rights are violated
    - Responsibilities of the government in order to protect the individual's rights to data
    - Responsibilities of private actors in order to avoid violating the individual's rights to data
    - Definition of community rights to data; informed consent with respect to those rights; adjudication, arbitration or other forms of resolution in the event of conflict between community rights and individual rights
    - Situations in which individuals' rights to their data may be derogated.
    - Rights of individuals and communities to access and benefit from the research findings that result from their own data.

    We submit that the framework needs to delineate the above requirements, measures, responsibilities and definitions in order to be a sound framework that respects the rights of citizens.

4. We note that this framework will be applied while India does not yet have a personal data protection law or anti discrimination law, although discrimination based on protected characteristics is prohibited according to Article 15 of the Constitution of India.

5. The Hon'ble Supreme Court's judgement in R. Rajgopal's[2] case has held that:
   "... The right to privacy is implicit in the right to life and liberty guaranteed to the citizens of this country by Article 21. It is a 'right to be let alone'. A citizen has a right to safeguard the privacy of his own, his family, marriage, procreation, motherhood, child bearing and education among other matters,"

   We submit that the framework should, therefore, explicitly lay out how Information Privacy (which involves the establishment of rules governing the collection and handling of personal data such as credit information and medical records), Bodily privacy (which concerns the protection of people's physical selves against invasive procedures such as drug testing and cavity searches), Privacy of communications (which covers the security and privacy of mail, telephones, email and other forms of communication) and Territorial privacy (which concerns the setting of limits on intrusion into the domestic and other environments such as the workplace or public space) of data principals are protected.

6. We recommend that the framework should operationalize "Privacy by Design" and "Privacy by Default" to all data principals, which calls for technical and organisational measures (TOM) already taken at the time of planning a processing system to protect data safety.

7. All data is interconnected and one crucial piece of information or data point can lead to a lot more of a person's personal life being revealed. For example, the mobile phone numbers, Aadhaar numbers and and pregnancy information of nearly 20 lakh women was leaked on the Internet in 2018[3]. The Aadhaar number served as a data point and provided information that included whether or not the woman does MNREGA work, how much she earned, if her child has a sibling, and if so, the school they went to, and her bank account number. From the perspective of the first and second degree effects of deanonymised data, we submit that the framework should address and provide protections to the social and civil rights of women, transpeople, LBGTQ+ people, religious and gender minorities, indigenous people, and other socially and economically vulnerable populations.

   Additionally, in S. Nambi Narayanan vs Siby Mathews & Others[4], the Hon'ble Supreme court has held that the *"...reputation of an individual is an insegregable facet of his right to life with dignity"*. Therefore, we urge the Committee that the framework should actively safeguard Data Principals, with a focus on people already navigating various social and economic vulnerabilities in the country, from the social implications of sensitive data being re-identified or deanonymised.

---

[2] Rajgopal Vs. State of Tamil Nadu 1995 AIR 264
[3] *AP govt leaks mobile, Aadhaar and pregnancy info of 20,71,913 women,* Vidyut, Medianama, 30 April 2018 https://www.medianama.com/2018/04/223-ap-govt-leaks-mobile-aadhaar-pregnancy-info, Last accessed 13 September 2020
[4] S. Nambi Narayanan vs Siby Mathews & Others Etc. CA 6637-6638/2018

8. We note that the conceptualisation of the state in the Constitution of India is based on the state as a facilitator of human progress. The Constitution in Part IV (Directive Principles of State Policy) lays down that the state should serve the common good and that the state is prone to excess. Hence, it is checked by effectuating both a vertical and horizontal separation of powers, as well as by investing every individual with fundamental rights that can be enforced against the state. Therefore, it is the duty of the state to put in place a data protection framework which, while protecting citizens from dangers to informational privacy originating from state and non-state actors.

9. We submit that the framework should enumerate the liability of the Data Custodian, Data Trustees and Data Trusts in case of re-identification, deanonymisation and loss of the fundamental right to privacy of Data Principals and communities.

10. Within the context of Article 14 (Right to Equality), Article 19 (Right to Freedom) and Article 21 (Right to Life and Personal Liberty) of the Indian Constitution, the framework should enumerate in detail the legal and ethical obligations on the part of Data Custodian, Data Trustees and Data Trusts to the Data Principal and the community to which the data belongs.

11. The framework should recognise that every Data Principal has the right to be informed of the data that is being obtained, whether directly or indirectly. If the Data Principal has given their data for a specific purpose but has not consented to its commercialisation, then it should not be used as such.

12. The framework should elaborate on the obligations on the part of the Data Custodian, Data Trustee and Data Trust to inform the Data Principal about the duration of storage, the rights of the Data Principal, the ability to withdraw consent, the right to lodge a complaint with the authorities and whether the provision of personal data is a statutory or contractual requirement. In addition, the Data Principal must be informed of any automated decision-making activities, including profiling.

13. The Hon'ble Supreme Court of India in the Puttaswamy judgement[5] has held that the right to privacy is a fundamental right flowing from the right to life and personal liberty as well as other fundamental rights securing individual liberty in the constitution. Privacy was held to have a negative aspect (the right to be left alone), and a positive aspect (the right to self-development). The sphere of privacy includes a right to protect one's identity. The right recognises the fact that all information about a person is fundamentally her own, and she is free to communicate or retain it to herself. The core of informational privacy, thus, is a right to autonomy and self- determination in respect of one's personal data. Additionally, in Maneka Gandhi v. Union of India[6], the right to life was considered not to be the epithet of a mere animal existence, but the guarantee of full and meaningful life. We submit that the framework should, therefore, consider the duty of the state under the Constitution to not amplify existing

[5] Justice K. S. Puttaswamy v Union of India WP (C) 494/2012
[6] Maneka Gandhi v. Union of India 1978 AIR 597

inequalities in the powers and privileges that adversely impact communities and demographics that are socially and economically vulnerable. We urge that the framework consider, address and propose protections against the risks of processing data that belongs to them.

14. Before considering data a "national resource", the committee should consider active dialogues and consultation with all stakeholders, including civil society, specifically in the best interest of Data Principals, not merely of the state or of businesses. The many communities and individuals whose data rights are being deliberated should be given the space to put their points of view across and decide the ways in which their data being processed is allowed to impact their lives.

15. In Section 5.1 (i) and (iii), the framework should:
    - Define and enumerate the meaning, scope and protection for the "best interest of that individual".
    - Define and enumerate the meaning, scope and protection of the "best interest of that community".

16. The right to privacy includes the right to control over one's body. The framework should focus on and address the socio-legal impacts of processing data from the Health sector. A patient would have to inevitably give details of their life to avail health care services. The very basic trust and understanding of doctor-patient confidentiality[7] will be compromised if health data gets deanonymised. The framework should consider and address the risk of deanonymisation would have on the access of socially and economically vulnerable populations to health care. For example: Due to existing social stigma, in the light of risk of loss privacy by deanonymisation, women may stop themselves from appraoching doctors for STD tests and abortions.

17. We further submit that the framework should examine all of its recommendations and propositions through the lens of:
    a. Article 12 of The Universal Declaration of Human Rights, 1948, which declares that a person's privacy, home, family or correspondence should not be subjected to any arbitrary intrusion or his honor and reputation should be attacked. Law confers on every person the right to be protected from such intrusion or attacks.
    b. Article 17 of The International Covenant on Civil and Political Rights, 1966 that lays down:
        i. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
        ii. Everyone has the right to the protection of the law against such interference or attacks.

[7] *Patient Confidentiality*, Rayhan A. Tariq; Pamela B. Hackert https://www.ncbi.nlm.nih.gov/books/NBK519540 Last accessed 13 September 2020.

18. The framework should elaborate how Data Principles will be protected within the context of Article 20(3) of the Constitution of India, which provides the right against self-incrimination to individuals.
19. Raw data does not exist naturally. Since most data sets are mixed and there are various degrees of overlap between personal and non-personal data, the framework should address the social and ethical implications of sharing mixed data sets as well as lay down regulations and procedures for processing mixed data sets.

20. The framework should call for a data protection impact assessment to be conducted when the processing of data could result in a high risk to the rights and freedoms of natural persons.

21. The framework should recognise and protect the right that Data Principals have to free, specific, informed and unambiguous consent, where the Data Principal is informed of their right to withdraw consent at any given time, which would lead to the erasure of their data. We urge the framework to enumerate how these rights would be delivered to Data Principals.

22. The framework should also formulate consent and its expression in such a way that the withdrawal of consent is as easy as giving consent.

23. The framework should recognise and protect the Data Principal's right to be forgotten where once their consent is withdrawn, links to their personal data, as well as copies or replicates of the personal data, must be erased.