CUTS International

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

Comments by Consumer Unity & Trust Society (CUTS International) on the Report by the Committee of Experts (The Committee) on Non-Personal Data Governance Framework (The Report) are set out below:

1. Overall Key Comments

1.1 The Report is a good resource to initiate discussion and serves as a food for thought on some of the impeding issues as far as non-personal data and its access is concerned. However, the proposed regulatory framework is not supported by any empirical evidence on the direct, indirect, intended, and unintended consequences of the proposed governance framework.

1.2 The Report does not clarify the scope and maturity of existing data market in India and thus, there could be a risk of over-regulation, which might create regulatory and compliance burden on existing and upcoming businesses. Most importantly, the report did not articulate what is the market failure that has substantiated the need for this regulation.[1] It also does not identify any concrete government/ regulatory failures which necessitate the need for a distinct regulatory architecture. While the Report does identify some issues to be addressed, it does not clarify why existing regulatory frameworks (and those in the process of being adopted) cannot be adequately strengthened to address such problems.[2]

1.3 While addressing the components and fundamentals of data in the digital economy is important, the Committee can first lay the principles focusing on citizens, equity, correcting power imbalance, addressing informal asymmetry and fixing accountability of players. However, such intervention is not an immediate necessity since the data market in India is at a nascent stage. Overall, to leverage the potential of data and the value that can be derived from it, an optimal regulatory approach would be to intervene once the market gains a certain level of maturity. Alternatively, it would be useful to first assess the dynamics of an emerging market, identify potential sectors and then design a pilot in one of the sectors such as health, etc. to justify and build evidence on the efficacy of such a governance

[1] Begoña Gonzalez Otero, Evaluating the EC Private Data Sharing Principles: Setting a Mantra for Artificial Intelligence Nirvana?, 10 (2019) JIPITEC 66 para 1.
[2] Mehta and Kulkarni, Kahlil Gibran and Data Regulation, August 2020, https://timesofindia.indiatimes.com/blogs/voices/kahlil-gibran-and-data-regulation/

framework. Global evidence suggests that non-personal data governance tends to be sector specific with some consistent overarching sector neutral guidance.[3]

1.4 Any regulatory approach or policy intervention must recognise the inherent distinctions between data markets and data platforms. Similarly, it is pertinent to assess if existing regulatory bodies such as the Competition Commission of India, etc. are better suited to address some of the issues pertaining to competition, entry barriers, monopoly, network effects, as identified in the Report. If such bodies have been unable to perform as per expectations as yet, the problem lies with their regulatory frameworks (and implementation thereof) for which designing a new regulatory framework cannot be a solution. Thus, such regulatory bodies would need to building their capacity and expertise to review entry barriers in data and platform markets.[4]

1.5 The Report argues that network effects create imbalances in the data industry. It states that certain businesses have gained a 'first mover advantage', which combined with network effects, creates significant entry barriers for startups and new entrants. In the Committee's view, therefore, this is the right time to set out rules to regulate the data ecosystem. The assumption that network effects automatically lead to monopolies is flawed. Digital markets are dynamic and consumers can switch to different platforms/ service providers with ease (multi-homing). Any *ex ante* regulation to 'curb' network effects without an assessment of harms to consumers is ill-founded. In any case, competition law and economics have the right tools to conduct this analysis and step in, as and where it is required. The legitimate state aim of reducing entry barriers for start-ups and reducing the networks of exploitation of data by large companies can be adequately addressed through competition law frameworks.

1.6 Finally, data does not have inherent value. It is only one piece in the chain of value generation; it is only when organizations process data for insights that value is created. Thus, any regulation of data that focuses on access/ sharing will not automatically correct any perceived imbalances. On the contrary, it may deter businesses from innovating and finding unique solutions to customer needs, particularly small and medium enterprises and start-ups, who may be forced to share the data they collect and process, with great difficulties. Also, as the Report notes, data is non-rivalrous.

1.7 We believe that regulatory intervention is premature and that the goals set out by the Committee can be best addressed through the existing competition law and IP regimes, the

[3] https://eudatasharing.eu/sites/default/files/2020-02/EN_AR%20on%20EU%20law%20applicable%20to%20sharing%20of%20non-personal%20data.pdf
[4] Ashok Kumar Gupta. "Digital Economy-Hitting the reset button on competition and regulatory governance". Special Address. CUTS International. New Delhi http://www.cci.gov.in/sites/default/files/speeches/CUTS.pdf?download=1

proposed data protection framework, incentivization arrangements, industry led codes of conduct and innovations like data exchanges and market places.[5]

2. Case for Regulating Data

The Report mentions that regulating Non-Personal Data (NPD) is essential to achieve the following:

1. *Come up with a set of recommendations such that India can create a modern framework for creation of economic value from use of Data. To generate economic benefits for citizens and communities in India and unlock the immense potential for social / public / economic value data.*

2. *To create certainty and incentives for innovation and new products / services creation in India. To encourage start-ups in India.*

3. *To create a data sharing framework such that community data is available for social /public / economic value creation*

4. *To address privacy concerns, including from re-identification of anonymised personal data, preventing collective harms arising from processing of Non-Personal Data, and to examine the concept of collective privacy.*

2.1 CUTS Comments

2.1.1 While the Committee is correct in articulating that data is a fundamental component in core-technological businesses, all economic sectors around the world are using data to address social and public administration issues. However, the Committee's justification to regulating data highlighting its significance is flawed. The problem statement needs to be defined, which must be backed by empirical evidence.

2.1.2 The Committee fails to articulate the general theory of recommending a regulation to facilitate data access– Why is regulation needed for Non-Personal Data? This question should be further sub-divided into – a. Why do markets by themselves not suffice? b. If there is to be government intervention, why does it take the form of regulation?

2.1.3 The Committee fails to articulate the market failure vis-à-vis Non-Personal Data that has necessitated the need for regulation. The issues pertaining to data access may be

[5] Some of these are documented by OECD, such as Estonia X-Road initiative; European Data Sharing space proposal, its Strategy for Data and Open Data Directive; Victorian Government data sharing policy; the Data Market Austria project; initiatives by International Data Spaces Association, the Ocean Protocol, and Findata. Many of these are covered in the report of experts on NPD governance framework in India. Some others include UK Geospatial Strategy; platforms like Vivli for sharing global clinical research data, iSHARE for sharing transport and logistics data; Zeotap; data marketplaces like Dawex; data exchanges like Convex; multi-owner data sharing and analytics platforms like MOSAICrOWN; and SWIPO for developing codes of conduct.

resulting from the normal dynamic of an emerging market, rather than a market failure.[6] Similarly, the Report fails to establish how market based interventions or voluntary incentives (self-regulation) for the data market to achieve similar objective have not been effective and efficient, which has posed the requirement for the government regulation/intervention.

2.1.4 The Committee also fails to articulate the linkages between NPD and existing and/or proposed policies that facilitate data sharing, openness of data, and data protection infrastructure in India and other sectoral regulations and intervention that may be effective in addressing some of the issues listed in the Report.[7]

2.1.5 The Committee also does not illustrate how existing policies or regulators have failed to address the inherent issues of data and digital economy, which has necessitated the need for NPD regulation. It is essential that the Report should create balance and coherence with other sectoral legislations.

3. Definition of Non-Personal Data and Key Roles

Define Non-Personal Data

1. *The Committee has defined three categories of Non-Personal Data – 1) Public Non-Personal Data 2) Community Non-Personal Data & 3) Private Non-Personal Data.*

2. *The Committee has also defined a new concept of 'sensitivity of Non-Personal Data', as even Non-Personal Data could be sensitive from the following perspectives – 1) It relates to national security or strategic interests; 2) It is business sensitive or confidential information; 3) It is anonymised data, that bears a risk of re-identification*

3. *The Committee recommends that the data principal should also provide consent for anonymisation and usage of this anonymized data while providing consent for collection and usage of his/her personal data.*

3.1 CUTS Comments

3.1.1 The Committee defines Non-Personal Data as any data that is not "Personal Data" as defined under the PDP Bill, or data without any Personally Identifiable Information. Overall, the definition is too broad and encompassing in its approach. There may be situations wherein the personal data (PD) and NPD are inextricably linked with each other and it might be difficult to clearly distinguish between PD and NPD, for instance, in the case of e-commerce data, which consist of mixed datasets. Thus, there is need to clearly define the specifics as to what constitutes NPD and not adopt an exclusionary definition

[6] Begoña Gonzalez Otero, Evaluating the EC Private Data Sharing Principles: Setting a Mantra for Artificial Intelligence Nirvana?, 10 (2019) JIPITEC 66 para 1.
[7] Ibid

as was done in the Report. To this end, there is a need to lay down an appropriate bright line test to clearly define NPD.[8]

3.1.2 The categorisation of NPD into three heads – Public NPD, Private NPD and Community NPD and their definitions are ambiguous and one-dimensional. There is a possibility of overlap between these different categories of NPD. Similarly, it might be difficult to categorise NPD in stated categories. The Committee failed to recognise and articulate the intersectional identities of people in the Indian community and seems to have considered community as a monolithic entity. For instance, a dalit woman living in rural India may showcase some inherent intersectional identities of a dalit community, women, and rural geography, etc. and thus identifying a community as a singular body may be a fragmented approach. Similarly, the definition and scope of community data is too broad, as it also seems to apply to foreign communities. This could cause the framework to be implemented overseas and thus non-feasible.

3.1.3 The Committee illustrates sensitivity of non-personal data (NPD), and links it to the sensitivity attributed to inherent PD. However, the perspective of relevant data principal (individual as well as community) about whether its data should be considered sensitive is missing. A similar observation was found in the Personal Data Protection Bill, 2019.[9]

3.1.4 Similarly, the scope of sensitivity also remains unclear given the linkages with underlying PD and the power to make such categorisations rests with the government. Thus, there is a need to relook at the categorisation of sensitivity and the scope for using a principle-based approach to establish levels of sensitivity and harms for both individual and community that may arise from illegitimate use of data or re-identification of data.

3.1.5 While the Committee has recommended consent mechanism for anonymization and usage of such data, however, the principles of purpose limitation, data minimisation, transparency, and accountability are pertinent and should be complied with. This could ensure transparency as data custodian should explain the purpose for which the data is being anonymised and that such data is utilised for the stated purpose only. In addition, the Report lacks attention on consent from users who have already left the platform, but their data is retained by the data custodian.

3.1.6 The Committee has also recommended that appropriate standards of anonymization be defined to prevent/minimise the risks of re-identification. Studies have suggested that the level of anonymization differs with techniques and tools, and thus the susceptibility of

[8] https://thewire.in/tech/non-personal-data-protection-anonymisation
[9] CUTS Submission to the Joint Committee on the Personal Data Protection Bill, 2019. https://cuts-ccier.org/pdf/submission-pdpb-2019.pdf

re-identification is changed.[10][11][12] Most importantly, over-anonymization can render datasets useless for further analysis or innovation.[13] Thus, there is a need to elaborate on the level and standards of anonymization that balances risks of re-identification and the utility of the dataset.

4. Defining Key Non-Personal Data Roles

Define Non-Personal Data Roles
1) Data Principal
2) Data Custodian
3) Data Trustees
4) Data Trusts

4.1 CUTS Comments

4.1.1 The Committee has defined data principals and categorised them. The Committee has also introduced data custodian as being responsible for the collection, storage, processing, use, etc. of data in a manner that is in the 'best interest' of the data principal/ community. However, the Report fails to clearly define "best interest".

4.1.2 The Reports also obligates data custodians to have a 'duty of care' while handling community NPD, however, the Report failed to provide parameters for risk assessment for attributing such duty of care. Thus, there is a need to formulate risk matrix for ex-ante risk assessment covering parameters such as unjustifiable collection, inappropriate use, security breach, etc. to assess tangible and intangible predictive harms to the community and individual data principal, if the data is mishandled.[14]

4.1.3 The obligations of 'best interest' and 'duty of care' must not be limited to mere principles, but should be enforceable and if these standards are not complied with, provisions should recommend appropriate action. Data custodians must be required to comply with a minimal set of obligations regarding purpose limitation, transparency, accountability, and data protection. Depending on the activities of data custodian, risk-based regulation should be implemented.

4.1.4 The Committee introduced data trustee to exercise the data rights of a data principal/community as the 'closest and appropriate representative body'. The example list indicates that most of the data trustees would be government entities. Where the government is the data trustee, it can also be a data principal or data custodian. Both data

[10] https://www.theguardian.com/technology/2019/jul/23/anonymised-data-never-be-anonymous-enough-study-finds
[11] https://theprint.in/opinion/india-has-to-toe-a-fine-line-in-defining-non-personal-data-between-public-interest-and-ipr/382149/
[12] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf
[13] https://academic.oup.com/idpl/article/10/1/11/5802594
[14] https://www.accenture.com/_acnmedia/pdf-35/accenture-the-ethics-of-data-sharing.pdf

custodians and data trustee are expected to perform different functions and while data trustee has an obligation of collective bargaining function, and thus, this could create a conflict of interest.

4.1.5 Multiple data trustees can have rights over the same NPD. If a data trustee is a registered NGO, it can lead to potential conflict amongst various groups with similar objectives and interests, prioritising their rights. In light of these, data trustees should be competent, unbiased and neutral parties, and thus comprehensive stakeholder consultation is a must. The interests of community should be prioritised over the interest of a data trustee.

4.1.6 The rationale for creating data trusts is unclear. The Committee stated that data trusts and infrastructure could be managed by public authorities or new neutral bodies. To this end, there is a need to ensure that concerns of conflict of interest, undue preferences are avoided in the management of data trusts. Similarly, the Committee has assumed that data trustee and data trusts will act in the best interest of the data principal/community, this proposition can be too idealistic. If data trusts are to be managed by the government while also holding community data and taking associated decisions on sharing such data, then the interest of community may get subservient. Thus, there is a need that the data trustee and data trusts should comply with adequate data protection practices, appropriate accountability, and transparency mechanisms.

5. NPD Sharing

Data Sharing Purpose

1) Sovereign purpose – Data may be requested for purposes of national security, legal purposes, etc.

2) Core Public Interest purpose – Data may be requested for community benefits or public goods, research and innovation, policy making, for better delivery of public-services etc.

3) Economic purpose – Data may be requested in order to encourage competition and provide a level playing field or encourage innovation through startup activities (economic welfare purpose), or for a fair monetary consideration as part of a well-regulated data market.

5.1 CUTS Comments

5.1.1 The Committee provides that the NPD could be requested for specified purposes – sovereign, core public interest and economic. However, the Report has provided little clarity on the scope of such purposes. For instance, detailed elaboration is required as to what does national security, law enforcement, legal and regulatory purposes entail for sharing NPD.

5.1.2 The Committee also failed to provide a process that is to be followed for data sharing for sovereign purposes. Similarly, the scope of 'wide range of societal objectives' for the sharing of NPD for core public interest purpose is ambiguous. In the absence of check and balances, transparency and accountability, any data sharing with the state for sovereign and core public interest purpose could create trust deficit and hurdles to achieve state's objectives. Thus, there is a need for greater clarity and transparency on these issues.[15]

5.1.3 An overarching governance framework encompassing all the sectors may just create discrete and innumerable policy implications for different sectors. Sectors that are increasingly using data and have specific requirement for data sharing can be prioritised such as health, agriculture etc. after comprehensive consultation with sector specific stakeholders.[16]

5.1.4 The requirement of mandatory sharing of data to open up competition for startups/ data trusts should not be considered as the first option. Businesses share data for mutual benefit determined by commercial negotiation and agreed contract terms. Any abuse of dominant position or anti-competitive conduct must be reviewed by Competition Commission of India (CCI), which have appropriate powers to enforce such remedies. However, the CCI also needs to reform and build its capacity and expertise on the digital economy. The Report also failed to find coherence with other regulatory bodies such as the CCI, which would be necessary to encourage competition and providing a level playing field in different sectors.

5.1.5 The Committee did not distinguish between data market and platform markets. As both of these markets have distinct issues, require different policy intervention, and thus are needed to be treated separately and differently. For instance, if the focus was on businesses dealing with large amounts of data and its access thereof, then CCI would be better suited to assess the data network effects, and if actions of such businesses are anti-competitive or are creating entry barriers for other market players. Similarly, if the issue pertains to consumer harm from data then such issue would need to be reviewed from the lens of data protection and other relevant policies.

5.1.6 A data marketplace provides for access to datasets, which may be static or live streams of new data.[17] Some examples of data marketplace may include but not limited to Microsoft Azure Marketplace, Xignite, Gnip, AggData, etc.[18] The Committee needs to establish such clear differentiation that would be relevant to India's market. Mandating data sharing as

[15] The principles of transparency and clarity are enshrined in Article 6 of EU regulation on the free flow of non-personal data. See, https://www.gs1.org/sites/default/files/infopackage-free-flow-non-personal-data.pdf
[16] van der Burg, S., Wiseman, L. & Krkeljas, J. Trust in farm data sharing: reflections on the EU code of conduct for agricultural data sharing. *Ethics Inf Technol* (2020).
[17] http://www.cs.unibo.it/~montesi/CBD/Articoli/MarketPlaceForData.pdf
[18] Begoña Gonzalez Otero, Evaluating the EC Private Data Sharing Principles: Setting a Mantra for Artificial Intelligence Nirvana?, 10 (2019) JIPITEC 66 para 1.

one solution fits all approach can turn out to be counterproductive in absence of understanding of these markets.

5.1.7 Finally, innovative products emerge when start-ups think of creative solutions to enter a market. Additionally, new entrants and start-ups with free access to data will have no incentive to invest in database construction and management. This will reduce their ability to maximize value from data and provide innovative business solutions, which is harmful to consumers in the long run. Mandatory data sharing may diminish returns for first movers, thereby reducing the incentive to take risks.[19] Moreover, forced sharing will discourage companies from investing in data analytics, an area identified as a national priority for the generation of IP under the National IP Rights Policy. Thus, a mandatory data sharing policy will go against the vision of a 'Digital India' and the goal of a USD 5 trillion economy.

5.2. Process of Sharing NPD

7.1: It appears that NPD sharing for sovereign purposes can be requested/ mandated by the state.

7.3(ii): The data trustees/ governments may themselves directly seek access to community NPD from private actors holding it, and place such data in appropriate data infrastructures or data trusts.

7.3(i): In case a request is made for sharing NPD for economic purpose and there is a dispute, the NPD Authority (NPDA) needs to evaluate the genuineness of such requests based on social/ public/ economic good and mandate sharing of data.

5.3 CUTS Comments

5.3.1 The Committee has provided for actors who are eligible to request sharing of data. However, the Committee did not provide the pre-conditions and process through which the data-requesting actors could make such requests. For instance, while the government and public authorities could request NPD for sovereign purposes, the Committee does not clarify if is it essential to first establish the principles of legitimacy, necessity, and proportionality before making such requests.[20] Alternatively, the Committee also did not clarify if any such requests would be subjected to judicial review.

5.3.2 In addition, the Committee has prescribed that Non-Personal Data Authority (NPDA) will be authorised to evaluate the genuineness of data sharing requests. However, the principles and benchmarks that the NPDA would use to assess such data sharing requests for the existence of social / public/ economic good are missing.

5.3.3 The Committee did not cite any empirical studies that may provide evidence towards the positive effects of mandating data sharing. On the contrary, it has been argued that

[19] Swire et al, *Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique*, Cyberspace Law eJournal, 2013, https://pdfs.semanticscholar.org/b826/c58ff279d3e6b3ae96583dcd5f023585b68b.pdf

[20] As laid down under the Puttaswamy judgement, while declaring the fundamental right to (informational) privacy.

mandating sharing of NPD may be value-destructive instead of leveraging value for digital economy.[21]

5.3.4 The Committee did not discuss the operating processes, costs and investments required for a company in making any data shareable, interoperable, and in machine-readable format. Access to datasets and its use are dependent on contractual and technical factors.[22] If the costs and investments are too high for companies without any return on investments, then it might also disincentivize the companies from collecting data. Thus, this recommendation needs careful scrutiny and empirical assessment. To this end, the Committee should engage in a cost and benefit analysis, and look at alternative mechanisms to address concerns regarding dominance in the market (and abuse thereof) as an alternate to mandatory data sharing.[23]

6. Data Sharing Mechanisms

7.4(iii)(a): Raw/factual NPD pertaining to community NPD that is collected by a private organization needs to be shared without any remuneration, subject to well defined grounds.

7.4(iii)(b): Where processing value-add is non-trivial with respect to the value or collective contribution of the original community data and collective community resources used, (or otherwise for reasons of overriding public interest) data sharing may still be mandated but on FRAND (fair, reasonable and non-discriminatory) based remuneration.

7.5(i): Indian citizens and organizations would have access to the meta-data about data collected by different data businesses.

The report also provides that algorithms/ proprietary knowledge may not be considered for data sharing.

6.1 CUTS Comments

6.1.1 Companies, including start-ups, may need to invest substantial resources to collect raw data including costs of software, hardware or proprietary interest of the collecting company. The Committee did not consider these costs adequately while framing the compensation model for data sharing. Most importantly, the Committee has failed to identify that anonymising raw personal data to raw NPD is also a value-addition, and thus removing remuneration from sharing raw NPD is inequitable and unfair.

6.1.2 India is a signatory to Trade-Related Aspects of Intellectual Property Rights (TRIPS) Agreement and thus, obligated to protect databases as literary work under the copyright

[21] https://www.medianama.com/2020/07/223-non-personal-data-nationalisation/
[22] Begoña Gonzalez Otero, Evaluating the EC Private Data Sharing Principles: Setting a Mantra for Artificial Intelligence Nirvana?, 10 (2019) JIPITEC 66 para 1.
[23] Kathuria et al, *Exclusionary conduct in data-driven markets: limitations of data sharing remedy,* Journal of Antitrust Enforcement, January 2020, https://academic.oup.com/antitrust/article/doi/10.1093/jaenfo/jnz036/5699250#191550816

law. Raw data is also protected under the copyright law if originality, efforts and creativity were involved in collecting and collating the data.[24][25] Under law, this assessment would need to be determined by courts and hence could open a Pandora's box for litigation on databases and copyrights. Thus, it is pertinent to detail and clarify any impeding issues with Intellectual Property Rights (IPR) and NPD.

6.1.3 Similarly, there is little clarity as to what constitutes raw data and value-added data and appropriate distinctions between them. The Committee did not provide standards for determining the scope and extent of value addition on the data and the process and parameters of assessing such value addition. The Committee must consider adequate compensation for companies to mandatorily share raw/factual data in addition to clarifying the scope and definition of raw data and value-added data.

6.1.4 The Committee has proposed to use FRAND based remuneration to access certain curated and analysed data. Such terms[26] have been seen in standard-setting processes in the telecom sector and are prescribed in case of licensing standard essential patents.[27] Moreover, if intellectual property were expropriated using FRAND obligations, then it would be subjected to three-step test[28], failing which would be a violation of TRIPS. The Committee must assess and clarify where FRAND terms are applicable, detailing such terms, process to design the same and how they could be applicable to non-rivalrous data or the data economy in general in coherence with applicable IPR laws.

6.2 Checks and balances for sharing NPD

7.6(i): Sensitive NPD may be transferred outside but shall be continued to be stored in India and critical NPD can only be stored and processed in India.

6.3 CUTS Comments

6.3.1 The Committee recognises privacy risks relating to NPD[29] and have identified collective harms. However, the Committee should comprehensively identify and define privacy harms for both the data principals – community and individual. Additionally, the relevance of mandating data localisation for NPD should be empirically assessed, coupled

[24] http://nopr.niscair.res.in/bitstream/123456789/3561/1/JIPR%2011%282%29%20125-131.pdf
[25] https://www.medianama.com/2020/08/223-nama-non-personal-data-copyright-competition/
[26] https://www.etsi.org/images/files/IPR/etsi-ipr-policy.pdf
[27] https://www.concurrences.com/en/glossary/standard-essential-patent-sep
[28] https://www.eff.org/files/filenode/three-step_test_fnl.pdf
[29] Even after Personal Data is anonymised into Non-Personal Data, the possibilities of harm to the original data subject(s) are not totally gone, as it is being increasingly recognised that no anonymisation technique provide perfect irreversibility. NPD report, point 4.5(iv). Mixing of different data sets may also lead to identification of data principals.

with ensuring adequate safety/protection of NPD. The assumed correlation between the location of NPD and data security may be misplaced.[30]

6.3.2 The Committee should clarify on relevant privacy and data protection obligations that entities handling data directories/ databases must be required to comply, irrespective of data location. The Committee should also elaborate on the grievance redress mechanisms for data principals (community and individuals) against any collective or individual harm. The grievance redress mechanisms should be user friendly, transparent, time bound, and enforceable. The Committee could refer to mechanisms by Central Public Grievance Redress and Monitoring System[31] and other best practices internationally to propose a comprehensive redress mechanism relevant for NPD governance.

6.3.3 Additionally, privacy and data protection/ security risks should be considered while evaluating data sharing requests as well. The Committee should evaluate merits in clearly defining and considering the application of principles of purpose limitation[32] and legitimate interests in data sharing.

7. Ease of Doing Business

7.1 CUTS Comments

7.1.1 In the backdrop of a Parliamentary Joint Committee assessing the draft Personal Data Protection Bill, 2019 (PDP Bill), the issuance of the Report calling for the regulation of NPD will strike nothing less than a body blow to incentives to invest in India. Businesses, which invest in India, will also be faced with two regulators overviewing "data", each regime with its own sets of compliance requirements leading to a significant adverse impact on ease of doing business.[33]

7.1.2 The Report also proposes that data businesses should be registered. Data collection and use is a routine activity, carried out by practically all businesses, governments, non-profits, etc. Registration will be an unnecessary burdensome requirement which hampers ease of doing business and harkens back to the restrictive licensing regimes typically earmarked for certain industries.

7.1.3 Data governance frameworks such as the EU GDPR have refrained from imposing registration requirements and moved away from infeasible obligations requiring data controllers to notify regulators before engaging in processing activities.

7.1.4 While the Report states that the registration process will be light-weight and digital, initial registration requires significant details to be provided. This includes rough data

[30] CUTS, Consumer Impact Assessment of Data Localisation, https://cuts-ccier.org/pdf/Findings_of_Consumer_Impact_Assessment_of_Data_Localisation.pdf
[31] https://pgportal.gov.in/Home/RedressMechanism
[32] As provided under the Personal Data Protection Bill 2019.
[33] https://telecom.economictimes.indiatimes.com/news/data-protection-authority-should-be-sole-data-regulator-in-india-cuts/76997738

traffic, cumulative data collected in terms of number of users, records and data, nature of business, kinds of data collection, aggregation, processing, uses, selling, etc.

7.1.5 The Report does not clarify the level of detail required. For instance, it is not clear if businesses can provide top-level categories (such as the fact that it collects traffic data, user details, financial details) – along the lines of information communicated through privacy policies, or if more granular details are needed. If more detail is needed, that it itself is a significant intervention without a pressing law enforcement, national security or public order need.

7.1.6 The Report suggests that the details required are similar to disclosures required by the pharma industry and in food products. This analogy does not account for a key difference within sectors – these are specialized sectors and drug manufacturers/ sellers and food businesses need licenses to operate. In contrast, data cuts across all sectors and in the Report's own framing, this registration is not intended as a license. Yet, it proposes extensive disclosures for data businesses.

7.1.7 The objective behind food and pharma disclosures is to prevent harm that can be caused from consumption of food, which is unsafe or ineffective/ poor quality medicines. Thus, food and pharma disclosures serve the larger goals of ensuring public safety, health and hygiene. There is a need for greater clarity on risks which data collection presents, and accordingly design proportional risk-based measures.

7.1.8 This may be of particular concern to small business and startups. A small organization may also trigger the data business threshold, if it happens to generate enough footfall to its website/ app. Registration requirements tend to impact small businesses more acutely, since they end up having to commit disproportionate resources to such compliances. While one of the core themes of the Report is to encourage domestic startups and small businesses, registration will only prove counter-productive to their interests.

8. Against Established Principles of Privacy, Competition and IP

8.1 CUTS Comments

8.1.1 In the Committee's view, the key reasons for regulating NPD are: (i) to create economic benefits by unlocking data's potential; (ii) to create certainty and incentives for innovation and new products/ services in India; (iii) to create a data sharing framework to make community data available for social, public and economic value creation; and (iv) to address privacy concerns to prevent 'collective harms' for processing of NPD.

8.1.2 However, each of these are already addressed by different regulatory regimes. The intellectual property regime (copyright law and patent protection) provides for protection of proprietary knowledge and also sharing of knowledge in a way that promotes business interests. The upcoming PDP Bill provides a comprehensive framework for privacy

protection, placing individuals at the center of all data-handling operations. The competition law framework looks to promote competition, including issues related to abuse of dominant position and entry barriers for new entrants. The need for a new regulatory framework is not made out and will only result in overlaps, running counter to the idea of ease of doing business. Excessive regulation may dissuade investment and innovation, and disproportionately affect small businesses and startups.

9. Overregulation and Overlap

9.1 CUTS Comments

9.1.1 The Report proposes setting up a separate non-personal data protection authority (NPD Authority), instead of allowing self-regulation by businesses regarding sharing of NPD, or submitting to the jurisdiction of sectoral regulators, like the DPA or the Competition Commission of India. However, creating yet another regulatory authority dealing in data is likely to only create a regulatory thicket and hamper the conduct of business in the country. It may become another parking slot for bureaucrats.

9.1.2 While the Report suggests that the NPD Authority should work in consultation with the DPA, Competition Commission of India and other sector regulators, as appropriate, so that issues around data sharing, competition, re-identification or collective privacy are harmoniously dealt with, experience suggests that this is more likely to lead to extreme policy uncertainty and avoidable large-scale litigations.

9.1.3 Instead of creating a separate Authority or legislation to govern NPD, if the goal is to correct perceived imbalances in the data and digital industry, this can be done through existing competition law provisions with no requirement for an additional regulation or regulator. Further, if a more 'enabling' rather than 'enforcement-only' role is envisaged, this can be achieved by suitably amending the competition legislation itself, rather than by creating a separate authority for that purpose.

9.1.4 The intellectual property regime (copyright law and patent protection) provides for protection of proprietary knowledge and also sharing of knowledge in a way that promotes business interests. The PDP Bill provides a comprehensive framework for privacy protection, placing individuals at the center of all data-handling operations. The competition law framework looks to promote competition, including issues related to abuse of dominant position and entry barriers for new entrants. The need for a new regulatory framework is not made out and will only result in overlaps, running counter to the idea of ease of doing business. Excessive regulation may dissuade investment and innovation, and disproportionately affect small businesses and startups.

****