RESPONSE TO THE

REPORT BY THE COMMITTEE OF EXPERTS ON NON-PERSONAL DATA GOVERNANCE FRAMEWORK

September 2020 | *Issue No. 104*

ESYA centre

ABOUT THE ESYA CENTRE

The Esya Centre's mission is to generate empirical research and inform thought leadership to catalyse new policy constructs for the future. It simultaneously aims to build institutional capacities for generating ideas which enjoin the triad of people, innovation, and value, consequently helping reimagine the public policy discourse in India and building decision-making capacities within government.

Esya invests in ideas and encourages thought leadership through collaboration. This involves curation of niche and cutting-edge research, and partnerships with people, networks, and platforms. Moreover, it prioritises multi-disciplinary research to engender "research clusters", through which practitioners and researchers collaborate.

ESYA centre

RESPONSE TO THE
REPORT BY THE COMMITTEE OF EXPERTS ON NON-PERSONAL DATA GOVERNANCE FRAMEWORK

We at the Esya Centre are grateful for the opportunity given to us by the Ministry of Electronics and Information Technology (MeitY) to respond to the Committee of Expert's Report on Non-Personal Data Governance Framework (Report). We appreciate that the Committee has attempted to set out a broad framework that seeks to regulate several facets of the use of Non-Personal Data (NPD) while identifying possible areas of concern.

In our suggestions, we engage with the Committee's key recommendations and identify areas which require greater clarity. We recommend actions that assist in creating effective regulation geared towards achieving defined goals and outcomes.

Part I contains the summary of recommendations, and **Part II** contains detailed analysis of the Report. We have structured our responses into 4 sections on Competition and Innovation, Ownership and Access, Privacy and Definitions, and the Regulatory Framework. Within each section, we analyse the key recommendations made by the Committee and propose alternatives. We have sought to engage with the Committee's recommendations on a first-principles basis and highlight areas which require greater conceptual clarity.

ESYA centre

PART I

SUMMARY OF RECOMMENDATIONS

We appreciate that the Committee sought to create a framework to regulate NPD that would enable the generation of economic value, promote innovation, and distribute the benefits accruing from NPD to communities the data was collected from. We find, however, that the framework proposed in the Report has the potential to exacerbate existing harms and lead to regulatory conflict. We frame our recommendations under 4 broad heads:

1. *Privacy*
   The proposed Data Protection Authority under the Personal Data Protection Bill, 2019 (PDP Bill) would be best placed to assess individual and collective privacy risks rather than the proposed regulator for NPD. The Committee's definition of a "community" is unspecific and overbroad and is difficult to operationalise. We recommend that the assessment of privacy risks is not included within the NPD framework, and that emerging concepts such as collective privacy are fleshed out in more detail before regulatory obligations are imposed on that basis.

2. *Competition and Innovation*
   The Committee should identify the exact nature of the market failure it seeks to address through mandatory data sharing. Further it must consider that the existing framework, in the form of the Copyright Act 1957 and Competition Act 2002, already provides the foundation for regulating competition and fostering innovation in digital markets. The Competition Commission of India possesses the necessary expertise to regulate ex-post concerns that may arise as a result of monopolisation, abuse of dominant position etc.

3. *Ownership and Access*
   The Report fails to engage with the existing commercial rights framework under copyright and trade secrets. The Committee does not anticipate conflicts, whereas there are clear legal-regulatory overlaps. While we agree with the need for a data sharing framework, we recommend a focus on voluntary, incentive-based sharing. Furthermore, the licensing mechanisms and exceptions established under copyright also provide an avenue to promote access to data.

4. *Regulatory Architecture*
   We find that the Committee's proposed regulatory framework does not lay down a clear mandate, is overbroad, and lacks necessary safeguards. We recommend that the Committee reconsiders the need for a separate regulator for NPD, that it clarifies regulatory ambits in areas of overlap with sectoral regulators, and that it focuses on frameworks to mandate collaboration between regulators.

PART II

DETAILED ANALYSIS

The Committee highlights the growing importance of data as an economic commodity and driver of social and political change. To this end, it cites the large volumes of data generated daily as well as the potential uses of data as an input for a range of emerging technologies, such as artificial intelligence and big data analytics. The Committee identifies three key issues linked to the data economy: imbalance in the market, incentives for innovation, and privacy concerns.

Privacy concerns stem from the fact that anonymised personal data is also classified as NPD. Anonymised personal data refers to information that contained personal identifiers, which have been removed through various forms of processing and scrubbing. However, extant literature clearly establishes that most processes of anonymization are unlikely to be irreversible. Hence, the use, sharing and processing of anonymised personal data is beset with privacy risks for individuals and communities. *The protection of privacy, individual and collective, is the first reason put forth by the Committee for the regulation of data*[1].

An imbalance in the digital market arises because foreign companies, primarily of US and Chinese origin, control vast amounts of valuable data. The Committee asserts that by coupling access to large volumes of data with the ability to process it using 'unprecedented computing power', these companies have acquired 'unbeatable techno-economic' advantages. As a result, new entrants, such as Indian start-ups, face significant challenges in the form of entry barriers and network effects. If this status quo continues, these companies are likely to acquire an imbalance of bargaining power vis a vis the Indian citizen, start-ups, and even the Government. Therefore, the second reason for regulation identified by the *Committee is the correction of market failure in the digital economy to ensure maximum public welfare and 'data sovereignty'*[2].

The need to spur innovation and foster new businesses in India is also associated with the correction of market imbalances. The Committee sees the creation of certainty and access in the form of 'economic privileges' over data, as key drivers of data-based innovation. *Clarifying the ownership of data and obligations for sharing of data, therefore, forms the third reason for regulation*[3].

The issues highlighted above are significant and need redressal. However, the Committee does not engage with ways to offset the potential harms it has identified. Moreover, it is not clear that remedies can be achieved only by granting a broad mandate to a new regulatory body. We explore the stated aims in more detail and examine the reasons put forth by the Committee to assess whether there are clear and cogent reasons to set up the proposed Non-Personal Data Authority (NPDA).

1. PRIVACY

The Committee defines NPD as all data that does not contain any information that can be used to directly identify an individual. In essence, NPD is all data that is not personal. Defined in this manner, NPD includes anonymised personal data. This is in line with the approach taken by the European Union, which is one of the few jurisdictions to regulate NPD[4]. However, this approach is not without concerns. For instance, both the PDP Bill and the Committee recommendations treat anonymised personal data as a form of NPD[5]. While such data does not contain any direct identifiers, no form of anonymization is irreversible. The Committee acknowledges this and identifies the possible privacy risks arising from re-identification of anonymised datasets[6]. It recommends that these concerns are addressed by treating anonymised personal data as the NPD of the data principal (as defined under the PDP Bill)[7]. It therefore

1 NPD Committee Report, p. 10.
2 NPD Committee Report, p. 23.
3 NPD Committee Report, p. 32.
4Article 3, Regulation for the free flow of Non-Personal Data in the European Union, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1807&from=EN.
5 Section 2, Personal Data Protection Bill, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1807&from=EN.
6 Luc Rocher et al., Estimating the success of re-identifications in incomplete datasets using generative models, Nat Commun 10 3069 (2019), accessible at: https://www.nature.com/articles/s41467-019-10933-3.
7 S. 2(14), Personal Data Protection Bill defines a data principal as: "data principal" means the natural person to whom the personal data relates.

requires the data principal to consent to anonymisation and the use of anonymized data. The NPDA will also be empowered to establish minimum acceptable standards for anonymization.

However, a perusal of the PDP Bill and its provisions show that the Data Protection Authority[8] (DPA) is perhaps better suited to handle these privacy risks, for the following reasons:

a) The DPA enjoys the specific mandate of securing privacy and inquiring into possible breaches[9]. The proposed NPDA, on the other hand, is geared towards realising the economic and social value of NPD.
b) The DPA is authorised to determine standards of irreversibility for anonymised data[10] and issue Codes of Practise detailing methods of de-identification and anonymisation[11].
c) Punishment for re-identification of anonymised data is prescribed under the PDP Bill[12]. Therefore, any prosecution arising from a re-identification event would have to be under the framework of the PDP Bill and not the legislation on NPD.
d) Allowing the DPA to manage the consent framework for personal data as well as anonymisation of such data and its subsequent use would result in more streamlined regulation.

We recommend that privacy concerns stemming from anonymised personal data are best dealt with under the framework of the PDP Bill. Since anonymised personal data has significant economic and social value, the Government could incorporate anonymised personal data as a category of personal data within the Bill.
In addition to the protection of individual privacy, the Committee identifies the protection of community or group privacy as an important aim of the proposed legislation. This is a positive development as big data analysis has the potential to reveal patterns and trends which can be used to target groups and communities[13]. However, the method of protecting group privacy proposed in the Report is unlikely to achieve the stated objectives:

a) The definition of a 'community' is broad and unspecific[14]. It is broad enough that virtually any group of individuals can claim that they form a community. Second, it is also possible that a person is a member of an ad-hoc community, without knowledge of such membership. For example, all individuals playing a particular multiplayer game at a point in time would form a community, as defined by the Committee. However, each player may not know the membership implications, for instance that their data could be controlled by a data trustee. Moreover, it is not clear what would happen if individuals are part of multiple communities with divergent interests, and if members of a community do not agree on what would be in their best interest. It is therefore doubtful whether this framing of a 'community' lends itself to the protection of group privacy.

b) Another set of concerns stem from the notion of data trustees, which are bodies mandated to manage data rights on behalf of communities. These bodies are likely to be the 'closest and most appropriate representative body' according to the Committee. However, identifying appropriate data trustees for each conceivable community is likely to be very difficult. For instance, which representative body will be chosen to be the data trustee for a community which comprises all users of an e-commerce platform? It is difficult to imagine that the MeitY or Department for Promotion of Industry and Internal Trade would be the appropriate body to protect the interests of such a large and varied body of consumers. Similarly, the capability of Municipal and Panchayat organisations to effectively manage data rights of their communities is questionable. Additionally, the Committee states that these trustees are to act in 'the best interest of the community', without elaborating on what such interest is and how the trustee can be held accountable. It also does not elaborate on what would happen in situations where a trustee is also the custodian of data. For example, the Ministry of Health and Family Welfare (MoHFW) may collect and process data on diabetes patients, and act as a

8 Established under s. 41 of the Personal Data Protection Bill.
9 Section 50, Personal Data Protection Bill.
10 Section 3, Personal Data Protection Bill.
11 Section 50, Personal Data Protection Bill.
12 Section 82, Personal Data Protection Bill.
13 Helen Nissenbaum et al., Privacy, Big Data, and the Public Good: Frameworks for Engagement, accessible at: https://www.cambridge.org/core/books/privacy-big-data-and-the-public-good/1ACB10292B07EC30F071B4AD9650955C
14 Community data is defined as: 'A community is any group of people that are bound by common interests and purposes, and involved in social and/or economic interactions.'

data custodian. At the same time, the Report states the MoHFW may act as trustee for data on diabetes in Indian citizens. While both entities are supposed to act in the best interest of the data principals, data trustees can also recommend obligations for data custodians. This creates a conflict of interest wherein the body wielding power to recommend sanctions is also an active participant on whom sanctions can be imposed.

The Committee acknowledges that collective privacy needs to be better defined and detailed in the future[15]. Hence, it is unwise to consider imposition of an array of obligations on the basis of a nebulous concept. As we discuss in Section 4, effective regulation requires clarity and certainty in both definitions as well as the mandate for the regulator. The objective of ensuring community privacy would be better served by multi-stakeholder bodies that represent vulnerable communities. A revised NPD framework should focus on identifiable groups, for instance a particular indigenous community in an area, which can evolve their own mechanisms for data governance, such as a data governance council. This will help create institutions which serve as conduits for groups managing their own data instead of it being held and managed by government[16].

The consideration of privacy within the NPD framework is vague and undefined. We recommend amendments to existing and proposed legislations, to ensure the protection of the privacy of Indian citizens.

2. COMPETITION AND INNOVATION

The Committee cites the potential for anti-competitive practices and the need for a level playing field as another reason for NPD regulation. The following paragraph from the Report provides a summary of this contention:

"Market transactions and market forces on their own will not bring about the maximum social and economic benefits from data for the society. Appropriate institutional and regulatory structures are essential for a thriving data economy and a well-functioning data society. The Committee's approach to regulating data, keeps such an understanding of data at its core." [17]

The Committee argues that certain companies have acquired positions of dominance in numerous data-based services. The proposed framework, therefore, looks to correct market imbalances in the form of network effects and barriers to entry by requiring open access to raw and meta-data generated by these large corporations. However, the approach adopted by the Committee does not address the following areas:

a) ***The nature of market failure in the data ecosystem and the regulatory tools best suited to remedy it:***
It is useful to consider whether the digital economy has precipitated competition issues that require redressal through such regulation. A range of scholars do not consider data and its collection, use and processing to be an antitrust problem, given that it is non-rival, ubiquitous, has a short economic lifespan and is highly substitutable[18]. While it is evident that certain digital platforms have acquired positions of dominance, it is not equally clear whether this is resulting in unchecked abuse of market power[19]. To this end, it is important to note that a several Indian start-ups coexist with the dominant players without a regulator. For instance, in the payments ecosystem, Indian start-ups such as PhonePe have outperformed products by global tech players, such as GooglePay[20]. Similarly, Zomato and Swiggy dominate the online food delivery segment, despite the entry of larger entities like Uber Eats. Research has also shown that regulation of markets with high uncertainty, which the data market can be classified as given the emerging nature of technology and the rules governing it, can often lead to a decline in innovation[21]. For instance, over-regulation of the telecom sector is one of the reasons for its current state of distress[22].

15 NPD Committee Report, p. 11.
16 Joshua Fairfield and Christoph Engel, Privacy as a Public Good, 65(3) Duke Law Journal (2015)
17 NPD Committee Report, p. 11.
18 Nestor Duch Brown and others, The economics of ownership, access and trade in digital data, JRC Digital Economy Working Paper 2017-01, accessible at: https://ec.europa.eu/jrc/sites/jrcsh/files/jrc104756.pdf.
19 The CCI in its primer on Dominant Position has stated: Dominance is not considered bad per se, but its abuse is. Abuse is stated to occur when an enterprise or a group of enterprises uses its dominant position in the relevant market in an exclusionary or/ and an exploitative manner., accessible at: https://www.cci.gov.in/sites/default/files/advocacy_booklet_document/AOD.pdf; Also see: The European Court of Justice recalled this key principle in a ruling when it said that: "...it is settled case-law that a finding that an undertaking has (...) a dominant position is not in itself a ground of criticism of the undertaking concerned. It is in no way the purpose of Article 102 (then 82 EC) to prevent an undertaking from acquiring, on its own merits, the dominant position on a market". Case C-209/10, Judgment of the Court (Grand Chamber) of 27 March 2012. Post Danmark A/S v Konkurrencerådet.
20https://www.businesstoday.in/technology/news/upi-game-gets-hotter-as-google-pay-and-phonepe-vie-for-market-share/story/413249.html.
21 Knut Blind et al., The impact of standards and regulation on innovation in uncertain markets, Research Policy Vol 46 Issue 1, February 2017, accessible at: https://www.sciencedirect.com/science/article/pii/S0048733316301743.
22 https://telecom.economictimes.indiatimes.com/news/opinion-high-priced-restrictive-entry-distorted-regulations-make-indias-telecom-sector-unattractive/75790943

However, situations may arise where control over a particular dataset hinders a downstream product from effectively competing with the entrenched player[23]. Similarly, mergers between companies with large datasets may result in monopoly formation[24]. In such situations, regulatory interventions may be necessary. The crucial question, therefore, becomes what form of regulation is required to level the playing field for all participants.

Some of the concerns discussed above can be dealt with by imposing positive rules that focus on responsible market behaviour. In other words, ex ante forms of regulation would help reduce barriers to access and information asymmetries[25]. Examples of such regulation include the establishment of platform neutrality rules to ensure that digital businesses engage with each other on a fair, reasonable and non-discriminatory basis. The Committee does well to identify the need for such ex ante regulations. However, the proposed data sharing mechanism does not resolve these issues as it suffers from a lack of clarity. The next section explores the problems with the data sharing mechanism in greater detail.

On the other hand, concerns from mergers, abuse of dominant position etc. would require ex-post interventions. The current legal framework, in the form of the Competition Act, 2002 (Competition Act), may be suited to this purpose. In 2019, the Competition Law Review Committee (CLRC) examined whether digital markets required a new antitrust framework. It found that the existing competition law was sufficient to cover a variety of issues caused in digital markets, including control over data and assimilation of market power.[26] However, this legal framework must be complemented by an effective and well-equipped institutional structure. The Competition Commission of India (CCI) is severely lacking on this front as a result of various factors, including a lack of requisite staff, constant delay in proceedings as well the gradual limiting of its mandate owing to judgements by the Courts.[27] A serious attempt at resolving antitrust in digital markets cannot be made without focus on improving CCI's capacities.

b) Unclear correlation between mandatory data sharing and innovation and value creation:

In mandating data sharing for data businesses, the Committee assumes that greater availability of raw and meta data will by itself spur innovation and help start-ups generate value. However, data is usually collected in a specific context, related to the commercial objectives that a collecting entity seeks to achieve[28]. Such data may be of limited use to Indian start-ups and the Government in the absence of the ability to derive value from it through refinement and processing. The Committee does refer to setting up cloud and data innovation labs and research centres. However, the Committee was granted a broad mandate by the MeitY[29]. By not engaging with the enabling and developmental role of regulation in greater detail, the Committee has missed an opportunity to spur the capacity building needed for Indian companies to compete at the global level.

The Committee's proposal of the selective sharing of data acquired from 'data businesses' with Indian companies and start-ups can negatively impact incentives for foreign companies to invest in collection and innovative use of data[30]. This is significant as the services sector in Inia relies on the investment of foreign capital[31].

We recognise the need for both ex-ante and ex-post measures to effectively regulate competition in data-based markets. However, we find that the current legislative framework provides for such measures. The Competition Act is well suited to implement ex-post measures, provided the CCI's administration and enforcement capabilities are strengthened. As we discuss below, the Copyright Act contains provisions which can be suitably adapted to enable a robust data sharing ecosystem.

23 Josef Drexl, Designing Competitive Markets for Industrial Data: Between Propertisation and Access, 8 (2017) JIPITEC 257 para 1, accessible at: https://www.jipitec.eu/issues/jipitec-8-4-2017/4636/JIPITEC_8_4_2017_257_Drexl.

24 Jacques Cramer et al., Competition Policy for the Digital Era, European Commission Directorate General for Competition, accessible at: https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf.

25 Nestor Duch Brown and others, The economics of ownership, access and trade in digital data, JRC Digital Economy Working Paper 2017-01, accessible at: https://ec.europa.eu/jrc/sites/jrcsh/files/jrc104756.pdf.

26 The CLRC also found that the framework under the Competition Act was enough to cover other related issues such as algorithmic collusion and online vertical restraints. See paras 2.2, 2.7, 2.10, 2.15, 2.16 of Chapter 8, pp 149-160, http://www.mca.gov.in/Ministry/pdf/ReportCLRC_14082019.pdf.

27 See, for instance: https://www.financialexpress.com/opinion/the-weakening-of-the-competition-law/2040371/.

28 Divij Joshi, Non-Personal Data: The 'Economic' Case for Regulation, Centre for Law & Policy Research, accessible at: https://clpr.org.in/blog/non-personal-data-the-economic-case-for-regulation/.

29 The Terms of Reference for the Committee are:

i. To study various issues relating to Non-Personal Data

ii. To make specific suggestions for consideration of the Central Government on the regulation of Non-Personal Data

30 The Impact Assessment accompanying the proposal for the EU's GDPR points out that sharing of publicly held data with select entities leads to distortion of competition in the market by providing certain companies with a competitive advantage.

31 https://dipp.gov.in/sites/default/files/FDI_Factsheet_12March2019.pdf

3. OWNERSHIP AND ACCESS

While the Committee sees the need to recognise certain rights over data and provide 'economic privileges' to data custodians, the following paragraph appears to capture an outmoded approach to data ownership:

"The term "ownership" holds full meaning only in terms of physical assets. Regarding intangible assets like knowledge and data, the term 'ownership' is relatively loosely employed to mean a set of primary economic and other statutory rights. For such intangible assets, many actors may have simultaneous overlapping rights and privileges. At times, such rights and privileges of different actors may not even interfere with one another, but this is not always so. It is therefore important that such rights and privileges related to Non-Personal Data are clearly defined and ascribed.[32]"

It is therefore not surprising that the Committee has failed to engage with the overlap between the proposed framework and the following rights:

a) The Copyright Act was amended in 1994 to grant recognition to certain kinds of computer-generated works. S. 2(o) was added to the Act for literary works to include computer programmes, tables and compilations including computer databases. This means that computer databases are protected as literary works and are eligible to be protected under Copyright law, provided they meet the creativity threshold for copyrightability.

b) Similarly, courts have held in various cases that datasets can also be protected as a trade secret, despite the fact that no legislation on trade secrets exists in India[33]. They have granted protection to trade secrets on the basis of contractual terms and principles of equity[34]. India is also a signatory to international agreements, such as the Agreement on Trade-Related Aspects of Intellectual Property Rights, which call for the protection of information that is secret or not generally known, has commercial value and has been subjected to reasonable steps to ensure its secrecy[35].

A failure to engage with existing commercial rights brings the data sharing mechanism proposed by the Committee into question. For instance, while the Committee does consider all proprietary data to be private data, it is unclear why the Committee assumes that raw and meta-data cannot be proprietary, in so far as Copyright extension can extend to even these datasets, provided they meet the threshold for originality'. Imposing mandatory sharing requirements for such datasets would then conflict with rights that exist in them. It is also pertinent that the Copyright Act contains provisions that allow for licensing rights emanating from copyright. This licensing mechanism can serve as the foundation for a robust data sharing ecosystem which allows companies to voluntarily engage and determine the value and permitted uses of their datasets, without negating their proprietary rights. The Committee should also consider whether existing models of collective rights management for Copyright can be adapted to the management of rights in data before proposing the creation of a novel framework. In addition to the above mechanisms under copyright, the Committee may also consider incentives in the form of standard form contracts or tax breaks that have been adopted in other countries to bolster data sharing and increase innovation by small and medium enterprises. (Refer to Annexure 1).

While the Committee's focus on increasing avenues for greater sharing of data is well placed, it must be balanced against the investment and effort put in by entities in data collection and processing. The Committee does provide for remuneration where data is shared for 'economic purposes'. However, the remuneration depends on arriving at an objective value of the data as well as an assessment of the degree of 'value add'. Estimating potential values of a dataset is difficult, given that a particular dataset can be put to innumerable potential applications[36]. There are also multiple approaches to quantify the value of datasets, as recognised in the Report, making it difficult to arrive at an industry-wide consensus on which approach would be most appropriate[37].

32 NPD Committee Report, p. 23.
33 John Richard Brady And Ors v. Chemical Process Equipments P. Ltd. and Anr [AIR 1987 Delhi 372]; Burlington Home Shopping Pvt Ltd v Rajnish Chibber (61(1995) DLT6)
34https://www.mondaq.com/india/trade-secrets/204598/trade-secrets-in-indiancourts#:~:text=There%20is%20no%20specific%20legislation,a%20breach%20of%20contractual%20obligation.
35 Surinder Kumar Verma, Protection of Trade Secrets under the TRIPS Agreement, and Developing Countries, 1 J. World Intell. Prop. 723 1998, accessible at: https://heinonline.org/HOL/LandingPage?handle=hein.journals/jwip1&div=37&id=&page=.
36 The Value of Data – Summary Report, Bennett Institute for Public Policy, Cambridge 2020, accessible at: https://www.bennettinstitute.cam.ac.uk/media/uploads/files/Value_of_data_summary_report_26_Feb.pdf.
37 NPD Committee Report, p. 7.

Hence, an approach that allows companies to mutually agree on valuation, in the form of licenses under the Copyright Act and/or voluntary data-sharing based on FRAND terms, is optimal. At the same time, any data sharing framework must also provide certainty on the protection of intellectual property (IP). In the past, certainty with regard to property rights has been undermined as a result of inconsistent policy making and inordinate delays in resolution of commercial disputes[38]. These shortcomings underpin India's consistently poor rankings on a host of indexes which measure economic freedom, competitiveness and protection of intellectual property. (Refer to Annexure 2).

The Report does not adequately address the ownership of NPD, as it fails to engage with the existing commercial rights under copyright and trade secrets. The proposed mechanism is likely to stifle digital economy investments in India, at a time when they are most needed. A voluntary approach based on creating incentives for data sharing needs to be considered to achieve the stated objectives.

4. REGULATORY FRAMEWORK

The Committee recommends setting up a dedicated regulator to govern NPD. While it considers alternatives, the Committee suggests that a new regulator is most optimal for a few key reasons – the separation of personal and NPD, the need to support start-ups, and to ensure data sharing[39]. It envisions the NPDA as a cross-sectoral regulator that can work in consultation with other regulators. The framework proposed by the Committee fails to account for several key regulatory considerations:

a) *Lack of clarity:*
Effective regulation is best achieved through clarity on the goals of regulation and the role of the regulator[40]. Per the Report, the primary driver behind the regulatory framework is the regulation of NPD such that its benefits accrue to Indian communities and businesses[41]. However, the broad framework suggested by the Committee contains concepts that are not explored in detail and will be difficult to operationalise. For instance, the concept of 'community data' as used in the Report is central to the framework but lacks specifics. As previously discussed in Section 1, the Committee has not clarified issues of what constitutes a community, how the same overlapping communities with differing aims or "best interests" should be reconciled, and that not all members of a community might agree on what would be in their best interest.

Similarly, in mandating data sharing for providing a level playing field, the Committee does not answer the questions raised in Section 2 above on the nature of market failure that is sought to be addressed, and on mandatory data sharing necessarily leading to more innovation by itself. Furthermore, as discussed in Section 3 above, in the context of mandatory data sharing, it is not clear how the framework proposed by the Committee would not contradict existing IP laws.

b) *Overbroad ambit:*
The Committee sees the NPDA as having a wide range of powers and responsibilities, classified under two broad functions: enabling and enforcing roles. Its proposed functions range from ensuring that data is shared to spur innovation by enabling data sharing for various specified purposes, ensuring compliance with regulation, undertaking risk evaluations of re-identification of anonymised data, supervising and addressing market failures for NPD, certifying technology standards, to adjudicating data sharing disputes and other unspecified functions[42].

Prescribing such a broad mandate creates regulatory overlaps, as discussed below, and makes it difficult to formulate accountability mechanisms since it can be difficult to measure outcomes and assess performance[43]. It also provides opportunities for "mission creep", wherein the exercise of regulatory power can exceed its intended ambit[44].

38 https://www.indiabudget.gov.in/economicsurvey/doc/vol1chapter/echap06_vol1.pdf
39 NPD Committee Report, p. 40.
40 OECD (2014), The Governance of Regulators, OECD Best Practice Principles for Regulatory Policy, OECD Publishing, Paris, Chapter 1, pp. 31-33, available at <https://doi.org/10.1787/9789264209015-en>.
41 NPD Committee Report, pp. 11-12.
42 NPD Committee Report, p. 41.
43 National Institute of Public Finance and Policy, Shubho Roy, Ajay Shah, BN Srikrishna, Somasekhar Sundaresan, 'Building State Capacity for Regulation in India', 10 July 2018, pp. 11-13, available at <https://macrofinance.nipfp.org.in/PDF/RSSS_building-state-capacity.pdf>; OECD (2014), The Governance of Regulators, OECD Best Practice Principles for Regulatory Policy, OECD Publishing, Paris, Chapter 1, p. 3, available at <https://doi.org/10.1787/9789264209015-en>.
44 OECD (2014), The Governance of Regulators, OECD Best Practice Principles for Regulatory Policy, OECD Publishing, Paris, Chapter 1, p. 32, available at <https://doi.org/10.1787/9789264209015-en>.

c) Regulatory overlaps:

The Committee views the functions of the NPDA as separate from existing regulators. However, the range of functions ascribed to the NPDA already fall within the ambit of multiple regulators and legal frameworks and is likely to create regulatory overlaps.

Authorities with conflicting and overlapping mandates can create regulatory conflict, as the jurisdictional battle between the CCI and the Telecom Regulatory Authority of India demonstrated[46]. Overlaps in regulatory ambit can also increase compliance costs for market participants, especially small businesses[47], and can increase litigation. Moreover, if there is to be a separate regulator that works in coordination with other sectoral regulators, it is essential to create mandated cooperation mechanisms that drive such processes[48]. Given that the proposed framework depends significantly on working with other regulators, this important aspect of good regulatory design is unaddressed by the Committee.

SECTORAL REGULATOR/ FRAMEWORK	OVERLAPS
CCI	As discussed in Section 2, the CCI is already tasked with ensuring competitiveness in markets and promoting consumer welfare and is empowered to do so with NPD as well. Competition authorities in other jurisdictions have also previously required data sharing in limited contexts to promote competition[45].
DPA	As discussed in Section 1, the line between personal and non-personal data are blurred and can change depending on context, and the DPA would be better placed to adjudicate issues of collective privacy and reidentification of anonymised data. Including this assessment under the ambit of the NPDA, whose mandate under the proposed framework is to undertake measures to derive economic value from datasets, might also create a conflict of interest.
Intellectual Property	As discussed in Section 3, there are overlaps with the copyright framework that are unaddressed in the Report. The objective of balancing the need to incentivise innovation with providing access to information falls squarely within the purview of IP law, and databases are protected under copyright. Allowing for more access to such resources would therefore have to be situated in the context of IP law.

45 The UK's Competition and Markets Authority, for example, proposed 'Open Banking' as one of the remedies to create competition in the retail banking market. See https://www.gov.uk/government/news/cma-paves-the-way-for-open-banking-revolution

46 OECD (2014), The Governance of Regulators, OECD Best Practice Principles for Regulatory Policy, OECD Publishing, Paris, Chapter 1, available at <https://doi.org/10.1787/9789264209015-en>.

47 India Business Law Journal, Karthik Somasundram and Sneha Jaisingh, 'Supreme Court settles turf war between TRAI and CCI', 3 April 2019, available at <https://www.vantageasia.com/supreme-court-settles-turf-war-between-trai-and-cci/>.

48 McGill R.K., Sheppey T.A. (2005) Regulatory Overlaps and their Impact. In: The New Global Regulatory Landscape. Finance and Capital Markets Series. Palgrave Macmillan, London, available at <https://doi.org/10.1057/9780230511989_5>

d) Need for safeguards:

While the Committee acknowledges the need to have 'appropriate safeguards' within the regulatory framework for NPD, it does not build in safeguards to prevent potential harms to individuals and communities. For instance, in exploring the concept of collective privacy, it recognises that NPD can provide insights that allow for collective harm such as discrimination[50], and states that safeguards are necessary. Unfortunately, the Committee does not explore any specifics. It also allows the State overbroad access to datasets[51], but does not address the potential surveillance harms that it would engender, such as discriminatory profiling of individuals and communities.

It is essential to design for and establish safeguards to prevent overreach by the State under a new regulatory framework. An important aspect of this is the design of an independent and accountable regulator[52]. Mandating cooperation mechanisms and engagement in regulation-making[53], instituting reporting and other transparency requirements[54], undertaking impact assessments[55], and building in regular review processes are some of the other best practices in regulatory design that the Committee could have addressed.

The framework proposed in the Report lacks clarity and will be difficult to operationalise. The mandate of the proposed NPDA overlaps with sectoral regulators and is likely to lead to conflict. The Committee has not focused on regulatory design and has not suggested appropriate safeguards . We recommend that the need for a separate regulator for NPD is revisited until such areas of regulatory design are addressed.

49 The UK and EU, for instance, often use MOUs. Formal MOUs are a way to deal with common issues – Ofcom and ICO MOU - trying to deal with nuisance calls together - joint regulatory framework. See also section on coordination, OECD (2014), The Governance of Regulators, OECD Best Practice Principles for Regulatory Policy, OECD Publishing, Paris, Chapter 1, p. 38, available at <https://doi.org/10.1787/9789264209015-en>.

50 NPD Committee Report, pp. 10-11.

51 NPD Committee Report, pp. 32-33.

52 See OECD (2014), The Governance of Regulators, OECD Best Practice Principles for Regulatory Policy, OECD Publishing, Paris, Chapter 3, available at <https://doi.org/10.1787/9789264209015-en>.

53 OECD (2014), The Governance of Regulators, OECD Best Practice Principles for Regulatory Policy, OECD Publishing, Paris, Chapter 1, pp. 38-39, available at <https://doi.org/10.1787/9789264209015-en>.

54 National Institute of Public Finance and Policy, Shubho Roy et al, 'Building State Capacity for Regulation in India', 10 July 2018, p. 26, available at <https://macrofinance.nipfp.org.in/PDF/RSSS_building-state-capacity.pdf>.

55 See the EU impact assessments at https://ec.europa.eu/digital-single-market/en/free-flow-non-personal-data

56 OECD (2014), The Governance of Regulators, OECD Best Practice Principles for Regulatory Policy, OECD Publishing, Paris, Chapter 4, available at <https://doi.org/10.1787/9789264209015-en>.

ANNEXURE 1: EXAMPLES OF COLLABORATIVE DATA SHARING MECHANISMS

Japan- Japan's Ministry of Economy, Trade and Industry has established a Contract Guidance on Utilisation of AI and Data, which provides factors on the basis of which data sharing agreements can be created or AI can be used. It is intended to be used as a reference for private businesses involved in data re-use or development of AI. It differentiates between three different types of data utilisation contracts: i) data provision contracts; ii) data creation contracts; and iii) data-sharing (platform) contracts. The Guidance provides in-depth explanations for fundamental concepts as well as rights and responsibilities of the parties. It provides examples of data utilisation contracts and outlines the main legal issues and the drafting processes for each contract type.
Japan's Certification System for data-sharing platforms provides government support to companies that want to share their data. This system includes a data request system, i.e. a system that allows data-sharing companies to request data that have been provided to relevant ministries and agencies. The government also provides support through tax incentives and administrative guidance, in particular. It can also revoke accreditation in some cases.

Netherlands- Netherlands' Dare-2-Share Cooperation Agreement aims at assisting entrepreneurs enter into agreements through honest and reliable processes by using the 'collaboration in innovation' phase, where data is shared between large and small companies. The initiative guides companies on the legal standards as well as national and international laws that parties need to incorporate in their agreements. The initiative has mainly been created for data sharing between larger and smaller companies. The model is comparable with standard form contracts in consumer agreements. Just the way consumers enjoy some level of protection after they have clicked 'I agree' without having read the numerous pages of conditions in English, a Dare-2-Share arrangement must offer small parties some security that they do not forfeit all their rights. Dare-2-Share is expected to significantly reduce the amount of time spent for setting out the starting points for data-sharing agreements.

Germany- The Industrial Data Space is a virtual data space that allows businesses to easily exchange and link data in a secured manner, that primarily protects the sovereignty of the data principal. They use standards and common governance models to facilitate the secure exchange and easy linkage of data in business ecosystems. IDS was funded EUR 5 million by the German Ministry of Education and Research between 2015 and 2018, and co-ordinated by the Fraunhofer Institute. Such a model provides a platform for creating and using smart services and innovative business processes, without compromising on privacy.

Europe- The EC has proposed principles for contractual agreements for sharing of non-personal data. They include transparency with regard to the data product, shared value creation by acknowledging that when data is created as a by-product several parties were involved in its creation. The parties must also respect each others' commercial interests, ensure undistorted competition and minimise data lock-in.

ANNEXURE 2: INDIA'S PERFORMANCE ON VARIOUS INDICES VIS A VIS BRICS + MEXICO

INDEX		RANK (SCORE)
Heritage Foundation: Economic Freedom Index		
a)	Brazil	144/180 (53.7/100)
b)	Russia	94/180 (61.0/100)
c)	India	120/180 (56.5/100)
d)	China	103/180 (59.5/100)
e)	South Africa	106/180 (58.8/100)
f)	Mexico	67/180 (66.0/100)
WEF: Global Competitiveness Index		
a)	Brazil	71/141 (60.9/100)
b)	Russia	43/141 (66.7/100)
c)	India	68/141 (61.4/100)
d)	China	28/141 (73.9/100)
e)	South Africa	60/141 (62.4/100)
f)	Mexico	48/141 (64.9/100)
Property Rights Alliance: International Property Rights Index		
a)	Brazil	62/129 (5.564/10)
b)	Russia	86/129 (4.989/10)
c)	India	55/129 (5.820/10)
d)	China	49/129 (6.033/10)
e)	South Africa	48/129 (6.071/10)
f)	Mexico	71/129 (5.228/10)

This document has been prepared by the legal research team at the Esya Centre. For any further contact, please get in touch with us at:

Esya Centre
A-281, Bhishma Pitamah Marg,
Block A, Defence Colony,
New Delhi -110049

www.esyacentre.org