CUTS COMMENTS ON THE REVISED REPORT OF THE COMMITTEE OF EXPERTS ON NON-PERSONAL DATA GOVERNANCE FRAMEWORK

Contents

Summary and Overall Key Comments

Consumer Unity & Trust Society (CUTS) wants to thank the Ministry of Electronics & Information Technology for providing a transparent platform for submission of suggestions and comments on the revised report of the **Non-Personal Data Governance Framework (the report).**

There have been several positive developments and changes in the revised report when compared to the first report by the committee of experts. It is appreciable that the committee has taken a relatively broader and open view and has clarified that data sharing between private entities is not under its ambit and also excluded data processors. Furthermore, the committee has tried to give much required clarity on mixed datasets and overlap with the Personal Data Protection Bill 2019 (PDP Bill). Given that there are several positive changes in the report intended to promote innovation and public benefits from data, CUTS would like to submit some recommendations on the revised report for the committee's consideration, to achieve these objectives. Briefly, these relate to:

- **Undertake cost-benefit analysis**: It is laudable that the report aims to foster innovation in public interest by enabling greater value realisation from non-personal data. However, the rationale to pursue this objective at this stage, incentives for suggested mechanisms to work, and checks and balances to prevent misuse, are not clear. In its current form, the report does not offer sufficient evidence to justify its rationale and assumptions, link them to the objectives, and consequently fails to make a convincing case for regulating non-personal data, in the manner it suggests. It also does not consider unintended consequences of its suggestions, particularly on consumers, start-ups, small enterprises, and the overarching vision to make India an economic powerhouse. The report needs to be placed appropriately in the Indian context, by considering market and policy maturity, state capacity, industry readiness, and infrastructure capacities of India. It should learn from India's experiences of superimposing a novel governance structure over weak institutional capacities negating optimal interaction, transparency, and accountability frameworks among citizens, industry, market, and the state. This necessitates undertaking a Regulatory Impact Assessment (RIA) of non-personal data governance framework for India which would require clearly defining the problem statement, intended objectives, analysis of costs and benefits of different regulatory options (including no-regulation, self-regulation, and co-regulation) on different stakeholders, and aid in selecting the most appropriate option, costs of which are likely to be significantly outweighed by benefits.

- **Ensure consumer welfare**: While the committee has tried to address concerns regarding overlaps with PDP Bill and empower consumers through consent mechanism, concerns remain regarding non-standardisation of anonymisation techniques and risk of re-

identification of data. The committee misses on internalising the problem of notice and consent fatigue as well as information asymmetry for consumers who may not know the purpose of anonymisation. Additionally, the 'opt-out' option instead of 'opt-in' mechanism tilts the governance of data under the current framework rather than PDP Bill, which may dilute privacy protection for consumers. In addition, there are concerns with respect to absence of clear transparency and accountability processes, risks of overlooking consumers' interests while making decisions on their behalf, apprehensions regarding profiling, exclusion and overcharging of consumers, complicated grievance redress mechanisms, and inadequate mandate for the Non-Personal Data Authority to act in customer interest. These issues need to be seriously considered and addressed appropriately, by the committee. A consumer-first framework which empowers and puts them at the centre of data governance, by providing practical mechanisms to consumers to enforce their rights needs to be designed.

- **Rationalise public interest purpose**: The committee seems to be making a case of 'public interest purpose' being achieved from sharing of High Value Dataset (HVD), however the way in which it has defined public interest is too broad leading to vague framing of its purpose. Here, the committee should be mindful that there can be externalities and unintended consequences such as stifling innovation, disincentivizing investments and increased business costs, particularly for start-ups. To address this, the committee should try to avoid the 'one size fits all' approach and should strive to achieve 'proportionality' between private costs and public benefits, examine 'necessity' of achieving public benefits through mandatory data sharing, while establishing the inability to facilitate sharing otherwise, and ensure 'reasonableness' of achieving such objectives in practice. This test can aid in rationalising the scope of public interest and laying down appropriate principles in this regard, which can protect interests of data principals, communities, and start-ups.

- **Reimagine community rights framework**: While the committee has tried to adopt a noble objective of establishment of community rights, it misses on recognising nuances, diversity, and overlaps in the existing community structures. This makes it difficult to define 'community' in a concrete manner, leading it to counteract the notion of community benefit, when the problem of 'identifiability' comes around. Additionally, to address the concern of data monopolies, the report seems to make an assumption that communities will be able to exercise their rights through data trustees that aggregate data sets in form of HVDs. This assumption does not take into account the possibility of creating another set of data monopolies, in form of data trustees, without adequate transparency. Conflict of interest concerns may also arise if data trustees, or their related parties, also act as data businesses or requesters. Moreover, the report gives a lot of discretion to data trustees without enough accountability. The committee should be mindful that without appropriate

transparency, accountability and redress mechanisms, such frameworks may not achieve the desired level of efficacy. The committee also appears to believe that existing communities will be able to identify, come together, appoint and direct a trustee to act for their benefit in a manner that power locked in data siloes is unleashed. This appears to be a wishing thinking given limited awareness and weak institutional frameworks around state-markets-industry-citizen interaction. Consequently, an environment for communities to communicate, come together, and interact with other stakeholders will need to be fostered as a pre-requisite for a community rights framework around data to truly work for their benefit. The committee also seems to ignore the pitfalls of adopting a public-private partnership (PPP) model in data governance by treating data as an infrastructure, and learning from our experience of PPPs in traditional infrastructure sectors, wherein there is immense evidence of profits being taken by the private sector, risks by public sector, and losses being left for citizens to incur. The idea to treat data like infrastructure and create digital public goods without building state capacity, governance structures around transparency, accountability, and grievance redress, and basic building blocks to enable common citizens benefit from such goods is problematic. Moreover, the state is increasingly pushing for delivery of public goods through digital means and is shutting out traditional non-digital means, in the garb of preventing leakages. Such digital only push has resulted in significant exclusion errors and substantial harm to citizens, and could be one of the reasons for rising inequality in the country, and substantially harm India's global standing. The report, which, in its current form, seems to be a step in the direction of creating such digital public goods, needs to learn from our experiences, and thus should focus on building capacities on the ground and with the state.

- **Experiment with voluntary frameworks which appropriately incentivise data sharing**: While the committee presents HVD as 'public good', it misses on prescribing appropriate incentive structures across the data value chain. It stipulates mandatory sharing of HVD with only caveat of adjudication by Non-Personal Data Authority (NPDA). This leaves the data custodian with underlying costs and disincentivises collection owing to risks of sharing the data with competitors. The incentives prescribed for data trustees and data custodians may not be sufficient to work in the interest of data principals and communities. To promote data sharing, enabling markets to design appropriate incentives, and fostering stakeholders to attain desired capabilities, sharing of open data sets should be prioritised for unlocking the value of data. This would also aid the industry develop voluntary data sharing frameworks, particularly at a sector level, given each sector has its own nuances. Given that the committee wants to promote sharing and usage of data by start-ups, small and medium enterprises, it should look at diverse incentive structures such as tax credits, viability gap funding, creating necessary infrastructure for data sharing and

usage, and capacity building for such start-ups. Even for data trustees, opportunities to create independent funding opportunities should be explored.

- **Minimise regulatory overlap and maximize regulatory collaboration**: The report has at several places clarified its jurisdiction, however, at the same time these clarifications are not necessarily with a clear understanding of scope and role of other regulatory agencies, or with an honest attempt to prevent regulatory overlaps. On top of the addressed overlaps with the PDP bill, there can be possible jurisdictional overlaps with Competition Laws, Intellectual Property Laws, sector-specific regulators, and with regulators like Competition Commission of India (CCI) and sectoral regulators. The CCI is expected to evolve its understanding, build internal capacities, deal with competition concerns in the digital economy. The argument that it hasn't done that yet for any reason whatsoever cannot justify the need for a new regulatory authority. These overlaps also may lead to possible violations of multilateral agreements which India has entered into, or bilateral agreements which is it intends to execute with different countries, for promoting exports and trade. The role of Non-Personal Data Authority itself is not clear. The report fails to provide a convincing argument of why a NPDA is required and why the functions envisaged for it cannot be efficiently and effectively discharged by the Data Protection Authority, the CCI, and relevant sector regulators at central or state level, either independently, or in collaboration with each other. There is a need to improve existing state capacity and empower existing regulatory institutions rather than creating new ones in the hope that they would perform. At the same time, there is a need to ensure better regulatory co-ordination through mechanisms like inter-regulatory teams, policy coherence and coordination units, which are increasingly becoming common across governments. It also appears that the committee is obsessed with making India a standard setter in global data regulation without acknowledging the state capacity constraints and infrastructure limitations in the country. As a result, a hurried approach to regulation may do more harm than good to the country.

Detailed Comments by CUTS International on the Revised Report by the Committee of Experts (the Committee) on Non-Personal Data Governance Framework (the Report) are set out in the sections below.

1. Case for Regulating Data

- *Considering the value generation capacity of the data economy, governments need to enable and regulate all aspects of data.*
- *To create a single national level regulation in India to establish rights of India and its communities over non-personal data, to address privacy, re-identification of anonymised data and prevent misuse of and harms from data.*
- *To create an enabling framework to ensure unlocking economic benefit from non-personal data for India and its people. And, to also create a data-sharing framework and provide certainty of regulations.*
- *The intended goal is to accrue the benefits of non-personal data processing to the community, create incentives for innovation and prevent collective harms*

Issues

1.1 While the objective of the report to derive 'public interest' from non-personal data (NPD) sharing is laudable, there appears to be broken linkages between the rationale, assumptions, evidence and objective of the report making the 'case of regulation of data' vague and unfounded. The report presumes regulation prescribing mandatory access as a silver bullet, skipping the building blocks in the middle.

1.2 In the current form, the report lacks specificity and clarity in addressing questions of 'what is the benefit of data sharing'; 'whose benefit the report is trying to achieve'; and 'how is the proposed framework optimally suited for India's data economy', leading to a vague objective and processes the report has built around it. **The need for regulation in public interest or what is often referred as 'public interest theory of regulation' is based on two underlying assumptions. First, unhindered markets have failed leading to problems of abuse by monopolies and externalities. Second, governments are benign and capable of correcting these market failures. In the current framework, while these assumptions are made, they are not substantiated with adequate evidence. This is leading to a command and control conception in the proposed framework without due consideration to complex causality of regulatory effects.**[1] There are also additional assumptions of seamless implementation and uptake of state-directed efforts and absence of adverse unintended consequences, which need to be avoided.

1.3 The committee seems to base its rationale on postulation that regulation will stimulate the nascent stage of data sharing practices in the economy in the direction of 'public interest.' However, here, the committee assumes that incentives to collect data are 'given' and that

[1] Peter Drahos, "The Regulation of Public Goods," *Journal of International Economic Law* 7, no. 2 (2004): 321–39, https://www.anu.edu.au/fellows/pdrahos/articles/pdfs/2004regulationpublicgoods.pdf.

businesses will continue to collect data not-withstanding governmental and other competitive business access to such data. This assumption forgoes the possibility of an inverse relationship between incentives for collecting data and sharing it for the purpose of 'public interest'.[2] Moreover, the wide scope of public interest including purely commercial business decisions like value addition, launch of new services, and incidental positive externalities of job creation may result in thinking that are data businesses already not operating in public interest, that they need to share data to meet the objective. Therefore, **proposing a regulation for mandatory sharing of NPD without any incentive structure may create a chilling effect on innovation and competition for existing data businesses and new entrants. This requires for close re-evaluation of the assumption and evidence on which the committee has based its 'case for regulation'.**

1.4 Moreover, the committee has also justified its case for regulation stating that governments around the world are realizing the need for regulating aspects of the data; however this argument needs to be evaluated in the Indian context. **The state capacity, infrastructure readiness, community consciousness about data rights, and stage of development of the Indian data economy may be different in terms of current and expected value realization from data and regulation could lead to unintended consequences without adequate evidentiary assessment.**

1.5 Countries which have also envisaged similar output from their frameworks of data sharing have based their rationale on existing use cases. **These use cases have helped them assess the kind of value and the associated benefits that data can generate for a community and based on that the frameworks have identified their approach towards data access. However, the report does not take into consideration the kind of market and policy maturity the European economy has over data, and appears to interested in leapfrogging over such steadily gained experience.** Further, Europe has been understanding and regulating data with policies as old as 25 years. It has achieved that level of policy maturity based on multiple previous regulations, including comprehensive personal data regulation, among others.[3] For example – the national data strategy which also forms the basis of the recently released Data Governance Act 2021 relies on use cases of data sharing; prevailing data governance models; and impact assessment to determine the industry readiness for data sharing. (see Annexure I for a snapshot of global experience). India does not have a comprehensive personal data protection legislation as yet, and aims to rush towards regulation of non-personal data.

[2] Niva Elkin-Koren and Michal S Gal, "The Chilling Effect of Governance-by-Data on Data Markets," *The University of Chicago Law Review*, 2019, 29

[3] https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en#:~:text=The%20GDPR%20is%20now%20recognised,process%20from%201995%20to%202018.

1.6 Looking at other jurisdictions, which the committee has claimed to achieve a balance between fostering an environment for innovation as well as protecting user rights, the report has lost focus on both these things and have been unable to convincingly secure either side of the balance. The committee must re-evaluate its approach in achieving the balance that it tried to find in the first place, taking into account externalities of legal systems as well as global markets into account, in an effort to strike a balance in such an evolving ecosystem.

Recommendations

1.7 To address these issues, the committee should take a step back assess the evidences of market failures; identify the problem clearly, examine the policy and industry maturity; analyse lacunae and gaps in existing policies and laws that the proposed framework aims to address, to establish a need for public law to establish community benefits in data. **Rationale for enforcing rights over NPD for public interest should stem from appropriate evidence.**

1.8 At this stage when India is pioneering its start-up ecosystem and is seeing a surge in new entrants in the market, it should be cautious that sub-optimal regulation has the potential to increase the cost of administration and compliance, can have unintended outcomes and limit the likelihood of achievement of the objective of the proposed framework. There is substantial evidence of such sub-optimal in traditional sectors, wherein small enterprises bear disproportionately higher cost of compliance, stunting their growth and impeding their ability to realise their potential. There is no need to repeat that template in digital regulation. **Therefore, it is of paramount importance to understand the impacts of any regulation, proposed or in operation, to achieve favourable outcomes, by analysing its costs and benefits on different stakeholder groups and ability to achieve its objectives. One such tool to build this understanding is Regulatory Impact Assessment (RIA). RIA is a process of systematically identifying and assessing direct and indirect impacts of regulatory proposals and existing regulations, using consistent analytical methods, like cost-benefit analysis**.[4] In practice before prescribing a new regulation the good practices of regulatory governance must be followed. For this, regulatory impact assessment should help to identify the need for new policy, designing the most effective and efficient policy design, regulatory or non-regulatory, or a mix, to ensure that resources of the country is used wisely. Analytically, this test is met if costs to society are justified by the benefits to society. The process of conducting RIAs takes account of the following essential steps [5]-

- Defining the problem and determining the cause

[4] https://cuts-ccier.org/regulatory-impact-assessment/, https://cuts-ccier.org/pdf/Summary_of_RIA_Initiatives_by_CUTS.pdf
[5] https://cuts-ccier.org/pdf/Regulatory_Impact_Assessment_Toolkit.pdf

- Identifying and understanding the baseline
- Developing regulatory alternatives through assessment of costs and benefits
- Selecting optimal alternative(s)
- Formal Public Consultation

1.9 The nature of the data economy is such that it is fast evolving and regulations will always play 'catch-up' with technology, therefore RIA methods like cost benefit analysis can give the committee and the government a solid ground for its future and current data policies. Additionally, this process would also ensure appropriate mechanisms for open, inclusive and more extensive consultations.

1.10 **Finally, it is imperative to take stock of current open data policies and other sectoral level data sharing initiatives, which may provide important lessons regarding the availability, demand and usability of data**. These policies should also be the starting point of developing voluntary data sharing habits before diving into prescribing mandatory sharing for public interest purposes onto the private sector. A similar approach has also been adopted by other jurisdictions such as the European Union (EU), United Kingdom (UK), Netherlands and Australia, which have first focused on open data policies and sectoral level data policies to make public sector data available (please see Annexure I and II for details on initiatves in other countries and learnings for India).

2. Definition of Non-Personal Data

- *When the data is not 'Personal Data' (as defined under the PDP Bill), or the data is without any Personally Identifiable Information (PII), it is considered Non-Personal Data.*
- *Based on data origins it will include data - that never related to an identified or identifiable natural person, such as data on weather conditions, data from sensors installed on industrial machines, data from public infrastructures, and so on. Secondly, data which were initially personal data, but were later made anonymous. Data which are aggregated and to which certain data-transformation techniques are applied, to the extent that individual-specific events are no longer identifiable, can be qualified as anonymous data.*

Issues

2.1 The committee has now expanded the definition of NPD to not just the data that is not personal data to any data that does not have 'personally identifiable information (PII)'. Here, the understanding of PII seems to be borrowed from PDP Bill, negating the lucidity associated with the definition of 'personal data' itself. The European experience with the application of General Data Protection Regulation (GDPR) has indicated that the

definition of personal data itself is very context specific. In this regard, EU Court of Justice in the case of *Peter Novak v. Data Protection Commissioner*[6] upheld the concept of 'relatability' in defining personal data which broadens the scope of definition making it more context specific. Similar observations were also made, in the privacy perception survey conducted by CUTS, involving in-depth interactions with around 2400 users, which highlighted the need to include user perception and perceived sense of users' intimacy and necessity of data in the test of 'identifiability'.[7] More recently, researchers have warned that considering the technological and jurisprudential evolution of the definition of 'personal data', a lot more data that was previously considered as NPD will come within the category of 'personal data'.[8]

2.2 **These reflections indicate that there is a possibility that the data which was once NPD maybe now be personal data depending on the context, leading to problems in creation of binaries. In such cases, it will be difficult to determine where the jurisdiction of Non Personal Data Authority (NPDA) ends and the Data Protection Authority (DPA) begins. This will result in more uncertainty related compliance obligations for businesses and increased risk for consumers.**

2.3 Such artificial distinctions and ambiguities regarding the scope of personal and non-personal data may enhance risk of privacy harms of consumers, increase compliance cost for industry, and nudge them to look for regulatory arbitrage.

Recommendation

2.4 The issues highlighted above points toward lack of policy maturity**. To address this, it would be beneficial if the committee formulates its approach after the implementation of the Personal Data Protection Bill 2019 (PDP Bill). This will help in establishing a 'rights based approach' from which a common understanding of values and principles can be internalised within the data economy. Apart from this, it is also important to develop further understanding of the data value chain to clearly distinguish and identify steps where the nature of data could change. This is important to avoid unintended privacy risks and harm to the consumers.**

[6] ECLI:EU:C:2017:994, para. 35.

[7] Objective: Engage with consumers on a pan India level regarding data and privacy protection on both, online, as well as offline platforms, from the government and private players alike. Expected Outcome: Policy reforms empowering consumers for data privacy and protection. https://cuts-ccier.org/cdpp/ and https://cuts-ccier.org/pdf/survey_analysis-dataprivacy.pdf

[8] Nadezhda Purtova, "The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law," *Law, Innovation and Technology* 10, no. 1 (January 2, 2018): 40–81, https://doi.org/10.1080/17579961.2018.1452176.

3. Interface between regulation for non-personal data (NPD) and Personal Data Protection Bill 2019 (PDP Bill)

- *The non-personal data regime applies to all data that is not personal data under the PDP Bill or which does not have any personally identifiable information.*
- *If the individuals whose data constitute the anonymized dataset are re-identified in any manner, such data would no longer be characterised as anonymized data to which the provisions of the PDP Bill will not apply. The dataset will be deemed to have been re-identified and once again fall within the purview of the PDP Bill*
- *The committee has proposed that to avoid overlaps with the PDP Bill, section 91 (2) and Section 93 (x) should be deleted.*
- *The Committee recommends that data collectors at the time of collecting personal* data *should provide a notice and offer the data principal the option to opt-out of data anonymization.*

Issues

3.1 It is appreciable that the committee has tried to address the overlaps between the previous report and the PDP Bill giving requisite clarifications on mixed datasets and applicability of PDP Bill in case of re-identified data. This definitely gives more clarity, however, uncertainty remains as the PDP Bill is not yet enacted. **This is specifically of concern as there are parallel yet conflicting narratives evolving around the PDP Bill and NPD. In an earlier press reporting on the PDP Bill, it was indicated that Joint Parliamentary Committee (JPC) is contemplating to also include NPD within the ambit of data protection, contrary to the current report. This necessitates for both the committees to work together.**

3.2 The committee rightly recognises that there is risk of re-identification of data, specifically through combining multiple non-personal datasets**. At the same time, it also encourages businesses to combine useful datasets to build solutions for public interests. This is an antithesis, going against the principle of data minimization. While the report provides for safeguards in the form of consent mechanism and applicability of PDP Bill in cases of re-identification, there needs to be further assessment how this balance between generating value and preserving consumer privacy could be attained.**

3.3 The committee prescribes opt-out options for data anonymisation through consent and notice mechanisms. However, this again negates the issue of notice and consent fatigue. CUTS privacy survey also highlighted this issue, that users do not read privacy policies

(notices) due to their length, legalese, complicated and unfamiliar language.[9] Despite the clear evidence of consent mechanism not truly empowering consumers, the committee further adds on to the information that the user is expected to process to formulate his/her consent. **Moreover, it also proposes for 'opt-out' rather than 'opt-in' option, which inadvertently tilts on the side of making the consumers' data available for sharing rather than being governed by the PDP Bill, as evidence suggests consumers typically go ahead with default choices. This also creates an information asymmetry for the users as the purpose of anonymisation cannot be specifically determined, which dilutes the objective of making informed and clear consent as has been prescribed in the PDP Bill.[10]**

3.4 Another issue that is being carried-forwarded from the previous version of the report is related to lack of standardization and uniformity in the anonymisation techniques, and the risk of over- anonymization effects. Data custodian, fearing the risk of regulatory non-compliance may over-anonymise the data impacting its inference quality and would affect its eventual use by the data requester (please also see Annexure III in this regard)**. Studies[11] and a detailed analysis conducted by the Article 29 Working Party while establishing standards for GDPR[12] have indicated that level of anonymization differs with different techniques and tools, thus the susceptibility of re-identification also changes. On the other hand, it is also observed that the over- anonymization of dataset can render it useless for doing further analysis and innovation.[13]**

3.5 At the same time, the committee has not further elaborated on the principles of collective privacy. While collective privacy is a new concept, it needs to be adequately discussed, even more so as the current framework specifically proposes for establishing community rights in data. These concerns will become prominent as algorithms become part of our everyday lives conducting profiling and processing functions putting vulnerable and marginalized communities at greater risks of harm from privacy compromise.[14]

3.6 Finally, many of these issues emerge from the lack of the policy maturity for making informed decisions on definition ambit of NPD, anonymisation techniques and consent architecture as there is no existing comprehensive data protection law which can inform

[9] Objective: Engage with consumers on a pan India level regarding data and privacy protection on both, online, as well as offline platforms, from the government and private players alike. Expected Outcome: Policy reforms empowering consumers for data privacy and protection. https://cuts-ccier.org/cdpp/

[10] https://cuts-ccier.org/pdf/submission-pdpb-2019.pdf

[11] https://www.theguardian.com/technology/2019/jul/23/anonymised-data-never-be-anonymous-enough-study-finds, 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] Marietje Schaake, "The Data Delusion," July 13, 2020, https://cyber.fsi.stanford.edu/publication/data-delusion. "Digital Dystopia: How Algorithms Punish the Poor | Technology | The Guardian," 2019, https://www.theguardian.com/technology/2019/oct/14/automating-poverty-algorithms-punish-poor.

practices and jurisprudence. **While in some sectors such as fintech[15] and health[16] in India, we have seen initiatives towards data sharing, we are still to draw learning lessons from these sectors. Furthermore, the open data initiatives have not yet reached requisite scale in India.** Many of the jurisdictions which have come up with data sharing frameworks specifically have personal data protection laws in place along with other sectoral level and public sector data sharing frameworks. For example, the Data Governance Act 2021 of the EU, specifically assesses the gaps in the public sector data availability and considers that as the starting point for increasing data availability. A**s a result, these jurisdictions have built jurisprudence and understanding of the industry readiness and established 'rights based approach' for better applicability of laws. (**also see Annexure I **)**

Recommendations

3.7 There is a greater need to understand the trade-offs and balancing risks which may result from increased data access and usage. Additionally, while the current framework has put the community at its centre, it is also important to align its effect on consumers who are starting points of data collection, and also part of communities.

3.8 While big data in being increasingly seen has source value generation, it also brings with it increased risk for consumers. This is specifically true in case of combined datasets, which present unknown risks. **For this, there is a need for exploration of innovative privacy enhancing technology such as Privacy Preserving Record Linkage, through which risks with combined datasets can be appropriately adduced.[17]** Thus, while we focus on economic value realization, a similar focus should also be placed in enhancing innovation to preserve consumer privacy. More generally, there is a need for greater thinking about consumer friendly and uniform consent architecture across data policies such as PDP Bill, Data Empowerment and Protection Architecture, the current framework, and sector specific initiatives on data sharing.[18]

3.9 Moreover, to deal with risks to the collective interest of vulnerable communities due to the uncertainty related to usage of big-data emanating from unpredictable algorithmic processing, the framework should prescribe ex-ante risk assessment parameters. **These should cover parameters such as unjustifiable collection, inappropriate use, security**

[15] Data Empowerment and Protection Architecture, 2020, https://www.indiastack.org/depa/

[16] National Health Data Management Policy , 2020 , https://ndhm.gov.in/stakeholder_consultations/ndhm_policies

[17] This technology identified and links records that correspond to the same real-world entity across several data sources held by different parties without revealing any sensitive information about these entities, Dinusha Vatsalan et al., "Privacy-Preserving Record Linkage for Big Data: Current Approaches and Research Challenges," in *Handbook of Big Data Technologies*, ed. Albert Y. Zomaya and Sherif Sakr (Cham: Springer International Publishing, 2017), 851–95, doi:10.1007/978-3-319-49340-4_25

[18]https://cuts-ccier.org/pdf/comments-for-niti-aayog-on-discussion-draft-of-data-empowerment-and-protection-architecture-2020.pdf

breach, etc. to assess tangible and intangible predictive harms to the community and individual data principals, if the data is mishandled, and should lay down clear accountability mechanisms.[19]

3.10 **In this regard, we could also be informed by the data sharing framework of Singapore, which recommends undertaking risk assessment** before data sharing on the basis of lack of control over the use of data, lack of control of change in exchange or platform modification, insolvency and reputational risks.[20] A similar approach has also been suggested in the Australian framework. (also see Annexure II). **The committee should formulate principles of anonymization for ex ante standardisation such that it creates balance between risks of re-identification and utility of the datasets, for establishing accepted level of risks of re-identification for a dataset to qualify as NPD.**[21] Some of the general best practices, in this regard as recommended by the report of Article 29 Working Party is taking a risk based approach to identify - new risks that could be created, identification potential of the anonymised dataset, envisaged release of data to third parties, appeal of the data set etc.[22]

3.11 Many of these recommendations could be adequately inculcated, after the implementation of the PDP Bill, which would bring out industry practices, consumer reaction and the capacity of the authorities to deal with privacy risk. **Thus, it is recommended that the committee, should wait before defining its approach towards consent and anonymization.**

[19] https://www.accenture.com/_acnmedia/pdf-35/accenture-the-ethics-of-data-sharing.pdf

[20] https://www.imda.gov.sg/-/media/Imda/Files/Programme/AI-Data-Innovation/Trusted-Data-Sharing-Framework.pdf

[21] https://academic.oup.com/idpl/article/10/1/11/5802594

[22] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

4. Data Businesses

- *A Data Business is any organization (Government or private organization) that collects, processes, stores, or otherwise manages data.*
- *A Data Business can be a data custodian or a data processor.*
- *A Data Business is a horizontal classification and not an independent industry sector. Existing businesses in various sectors that collect data will get categorized as a Data Business.*
- *Data business above a certain threshold is required to register and share meta-data into the meta-data directory managed by NPDA.*

Issues

4.1 While the committee has stated that sharing amongst private entities is not in scope of its jurisdiction, **the ambiguities surrounding the data sharing mandates and compliance requirements for data businesses remain ambiguous and unfounded.** The committee in this version of the report, has tried to elaborate the criterion determining threshold requirements for registration, however the ambiguity about necessity to do so still remains. The threshold requirements such as percentage of revenue or number of consumers on the platforms should be adequately specified, and clearly linked with the rationale that is intended to be served by such registration. This will lead to uncertainty for businesses.

4.2 Further, the parameters to define and classify data businesses are not specified, indicating the data business category is synonymous with the "significant data fiduciary" in the Personal Data Protection Bill (PDP Bill). This way the combined compliance requirements from the PDP Bill and the proposed framework may deter businesses to reach this threshold leading to stifling of innovation.

4.3 Additionally, **the registration and subsequent disclosure requirements does not provide the granularity to threshold of the details required to be complied by the businesses**. Moreover these disclosure requirements may be onerous and unnecessary for some businesses. Data business is a horizontal classification and includes all sectors, in such a case for many businesses which are not per se data intensive, and may only collect and process data as by product would still have to comply with registration requirements. This creates uncertainty and may put greater compliance burden on small businesses and startups. **Moreover, a small organization may also trigger the data business threshold, if it happens to generate enough foot-fall to its website/ app. This will impact small businesses more acutely, since they end up having to commit**

disproportionate resources to such compliances which would ultimately lead to disincentives in reaching such scale of business operations.[23]

4.4 **This goes against one of the core themes of the Report, to encourage domestic startups and small businesses, as registration will only prove counterproductive to their interests and adversely impact 'ease of doing and running of businesses', an area on government is laying significant stress**. Even the General Data Protection Regulation (GDPR) in the EU has not stipulated such registration requirements.

4.5 Moreover, while the committee has defined meta-data, the requirement of mandatory sharing of meta-data, completely negates the cost of collection of such data and involvement of creativity in determining even the 'fields of collection of data' on which businesses may have built competitive advantage. Data fields of the meta-data may themselves be commercially sensitive for some businesses.[24] In such cases, 'one size fits all' approach of sharing all data fields, should be re-evaluated and fixing of certain incentive measures is also required.

4.6 In this context, the issue of mandatory access to meta-data should be read with its eventual purpose of extraction of high value datasets (HVDs) on mandatory basis with only caveat of adjudication by NPDA. Thus, looking at it holistically, it may divulge commercially sensitive information to competitors who can eventually extract the data through data trustees in the form of High Valued Datasets (HVD), thereby disincentivising businesses to collect data and undertake innovation.

4.7 Another issue emanates from the responsibility of NPDA to manage meta-data repository, and the underlying **assumption that the authority will be capacitated to maintain adequate security and also ensure findability for this data repository. In order to resolve this, the first step should be to assess infrastructure capabilities, state capacity, technical capabilities in the country.**

4.8 Such assessment would reveal areas wherein improvements are required prior to attempting regulation including mandatory data sharing.

Recommendation

4.9 These issues require a complete cost-benefit analysis to understand the cost additions to the data business owing to the current framework and its effect on innovation, ease of doing business and 'public interest' as envisaged by the report. It would also be beneficial to determine the risks that registration measures are intended to address before reaching threshold a criterion and disclosure requirements. As has been stated before, it is imperative that we tread carefully before prescribing for any regulatory compliances as this may stifle an emerging sector.

[23] https://cuts-ccier.org/pdf/comments-on-the-report-by-the-committee-of-experts-npd.pdf

[24] Jane Greenberg, "Metadata Capital: Raising Awareness, Exploring a New Concept," *Bulletin of the Association for Information Science and Technology* 40, no. 4 (2014): 30–33, doi:https://doi.org/10.1002/bult.2014.1720400412

Establishing Rights over NPD

5. Non-Personal Data Roles – Community

- *The committee has defined community as any group of people that are bound by common interests and purposes, and involved in social and/or economic interactions. It could be a geographic community, a community by life, livelihood, economic interactions or other social interests and objectives, and/or an entirely virtual community.*
- *The Committee recognises that, in the absence of a data principal for non-personal data, a community can exercise these rights over non-personal data to derive economic and other value and maximizing data benefits, and prevent harms to the community.*
- *Community will exercise their rights over NPD, through data trustees.*

Issues

5.1 The committee has presented a community rights-based model over non personal data, which is a progressive move compared to the ownership model which was suggested in the previous report. While the committee's intention to use data for common good is commendable, the report has taken a flawed approach to achieve that.

5.2 The committee has suggested conflicting views on how it seeks to understand and treat NPD. To suggest a community-based approach, the report cites constitutional and judicial precedents, thereby equating data with 'material resources' that should be distributed for the common good. The report itself identifies that there are multiple ways to understand and treat data. The community rights understanding of material resources stems from the value that the community understands from such a resource, however, data is different from other material resources. **The value of data is not pre-determined, and its use only becomes apparent when organisations collect and process for providing services to the community**. Thus, **the committee must re-evaluate its view of data and then decide on ways to regulate data.**

5.3 Additionally, it has been assumed by the committee that to exercise rights over the non-personal data communities will come into existence organically. In this regard, **the committee must be mindful that with the extraordinary level of diversity and complexity in Indian society, it will be difficult for people to relate with each other as these communities are not defined properly. In addition, citizens typically have multiple identities depending on their location, occupation, gender, social and economic standing. The identities and roles change, depending on context and other individuals they are interacting with, such as family, friends, society, among others. Consequently, individuals may part of different communities at any given point of time,** thereby making it difficult to link them to specific communities. This

could defeat the purpose for which communities are intended to be empowered by the committee, as the notion of organic self-identification by the group for forming HVD might be far-fetched in the Indian context. It is, therefore, crucial to further analyse this as community rights in data differ from the existing community rights in other resources such as forests or land, wherein there is an organic identification of a community because of the apparent utility being derived from such a resource, and limited awareness among citizens about rights in their data.

Recommendation

5.4 **It will be beneficial if the committee re-evaluates its jurisprudential and legal basis of establishing community rights through understanding the differences between traditional notions of 'identifiability' of community with a resource and that related to data. It is also equally important to internalise that the community identification with data as a resource is a gradual process and as people will understand privacy rights and importance of data communities will emerge on their own and may not necessarily require regulatory stimulation. To nudge this process, open data practices and voluntary data sharing mechanisms could be explored.**

6. Data Custodian and Data Processor

- *The data custodian is an entity that undertakes the collection, storage, processing, use, etc. of data. Typically, it is the data custodian that has a relationship with the consumer from whom data is collected.*
- *Data processor means a company that processes Non-Personal Data on behalf of a data custodian*

Issues

6.1 The committee has provided definitions in order to distinguish between the Data Custodian and Data Processors. The report specifies that a data custodian has a responsibility in data stewardship and has a 'duty to care' regarding the handling of non-personal data, to ensure that no harm to the community or an individual comes from sharing any data while protecting both the accidental or active misuse of non-personal data. **However, it does not clearly define these distinctions and neither does it provide any clarification on what the committee means by these terms. The committee should provide context and definitions for both these terms with illustrative examples like the report has done with many other concepts**.

6.2 The report also talks about when data processors will not be considered data custodians during the time they are processing the data and will not be expected to share any data in that period. However, this exemption does not apply where the data processor collects, stores and processes NPD as part of its other key business operations, and not on behalf of another data controller/fiduciary posing risk of excessive regulation.

Recommendation

6.3 The committee must consider specifying the way data custodians can approach responsibilities of 'duty of care' using a risk-based approach while also setting criteria where the data custodian can decide on the possible risks of sharing any non-personal data**. In this regard we could also be informed by data sharing frameworks adopted in Singapore, which specifies the principles through which 'duty of care' and trust could be ensured between parties involved in data sharing such as** transparency, accessibility, fairness and ethics (proper data protection measures), accountability, security and integrity (also see Annexure I).

7. High Value Datasets and Data Trustees

- *An HVD is a dataset that is **beneficial to the community at large** and shared as a **public good**, subject to certain guidelines pertaining to the management of an HVD and data sharing.*
- *The Committee has defined a data trustee as an organization, either a Government organization or a non-profit Private organization (Section 8 company / Society / Trust), that is responsible for the creation, maintenance, data-sharing of High-value datasets in India.*
- *Data trustees have a responsibility towards responsible data stewardship and a 'duty of care' to the concerned community in relation to handling non-personal data related to it.*

Issues

Is there a 'public interest purposes' in the context of HVD?

7.1 The committee has prescribed for sharing of high-value datasets (HVD) that is beneficial to the community at large and serve as a public good. Expanding on this, the committee has highlighted certain areas and purposes under para 7.6 of the report which includes creation of new businesses, jobs, value added services or applications and also specifies for 'and other' purposes. **The way in which 'public interest purpose' is defines, gives an ostensibly wide mandate to cover all kinds of purposes within it leading to a vague problem statement without clear link between targeted community benefit and purpose of use**.

7.2 **In fact in the current form, it appears that, under the garb of public interest, mandated sharing of HVD amongst private entities through data trustees would be undertaken for both 'for profit' and 'non-profit purposes'**. No fixed meaning has been ascribed to 'public interest' in Indian jurisprudence in other areas such as natural resources, right to information and intellectual property rights etc.

7.3 The Supreme Court in the case of *Bihar Public Service Commission v. Saiyed Hussain Abbas Rizwi* referred to the definition of public interest stipulated by Black's Law dictionary i.e. "the expression "public interest", like "public purpose", is not capable of any precise definition. It does not have a rigid meaning, **is elastic and takes its colour from the statute in which it occurs, the concept varying with time and state of society and its needs.** It also means the general welfare of the public that warrants recognition and protection; something in which the public as a whole has a stake.[25] In another case of land expropriated the court stated that *"[We] must examine these questions very carefully when little Indians lose their small property in the name of mindless acquisition*

[25] (2012) 13 SCC 61

at the instance of the State. If public purpose can be satisfied by not rendering the common man homeless and by exploring other avenues of acquisition, the Courts, before sanctioning an acquisition, must in exercise of its power of judicial review, focus its attention on the concept of social and economic justice. While examining these questions of public importance, the Courts, especially the Higher Courts, cannot afford to act as mere umpires."[26] **These rulings indicate that while no fixed definition can be ascribed to public interest, the risk of its misuse through expropriating resources can lead to adverse consequences for the very beneficiaries it is intended to help; in the present situation those beneficiaries are smaller start-ups and businesses, and eventually the citizens to whom the data relates to. The court, in the aforementioned matter, also stressed upon the need for exploring alternative mechanisms to achieve stated objectives.**

7.4 Furthermore, as has been indicated earlier, regulations for public interest should emanate from first establishing current market failure and identifying the problem statement and then assessing the current government capacities and capabilities of citizens to interact with the government to ensure that their interests are taken into account. In the report, **firstly, the committee assumes that there exists market failure and existing need of data sharing for public interest without any evidence of current practice and gaps in the market**. In this regard, we should be mindful that without clear moral necessity of sharing data as public good, there may emerge harms from unequal power dynamics and bargaining powers hampering innovation, data collection and processing.[27] **Secondly, there is also an assumption that India has the policy maturity, regulatory capacity, and infrastructure capability, without accounting for learning lessons from current open data and other existing data sharing policies**. Creating heavy handed regulation, without clearly establishing this criterion to mandatorily share data will lead to unintended consequences.

7.5 **Therefore, without any specific criterion or purpose limitation for assessing 'public interest', uncertainty would be created for businesses, which would fear compliance. Thus, instead of creating an enabling eco-system, it might kill existing or emerging data markets. In this regard, lessons may be learned from other sectors such as electronics, capital goods, electric vehicles, renewable energy, which despite the government push through regulation and schemes were not able to tap into the opportunities due to inherent lack of infrastructure, sub-optimal contract enforcement, weak R&D, and innovation environment.**

[26] Radhy Shyam(D) Thr. Lrs & Others vs. State of U.P. & Others, (2011) 5 SCC 553

[27] Taylor L. 2016 The ethics of big data as a public good: which public? Whose good? Phil. Trans. R. Soc. A 374: 20160126. http://dx.doi.org/10.1098/rsta.2016.0126

Is data a 'public good'?

7.6 The economics around data is still evolving and different jurisdictions are giving varied resource attribution to data. For example, UK is now proposing to treat data as an infrastructure,[28] and it has also classified data as an 'experience good',[29] while the US considers it as a capital asset. India through the current framework has ostensibly stipulated HVD as 'public good'.

7.7 Conceptually public goods are non-rivalrous and non-excludable in nature. The form in which non-personal data currently exists with private companies makes it non-rival and yet excludable due to existing intellectual property rights and its commercial value for businesses. This makes data a 'club good' or 'impure public good'. Thus, in order to transition this data from 'club good' to 'public good', as intended by the report, the costs and associated externalities needs to be closely assessed.

7.8 The committee also prescribes a legal explanation of equitable distribution of data, stating that it may be considered as a 'material resource' and its equitable distribution should be ensured under Article 39. However, considering data as other natural or material resource would be flawed. **Studies and experts have indicated that the nature of data is different from other natural resources such as 'oil', because of the way in which the value is derived from data. This is because data itself 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.[30] Thus, prescribing similar regulations such as land acquisition will not be efficient in the case of data.**

7.9 This is specifically important as ex-ante assessment of social benefit accruing from data is difficult. While the report intends that the benefits derived from data access would be available to a larger community, however, certain excludability may emerge in instances of data usage by a business or for businesses. **Thus, 'one size fits all' to consider all HVD as a public good in all circumstances need to be re-considered**.

7.10 An alternate interpretation underlying the notion of the public good is to consider data as infrastructure**. However, even if we envision data as a public infrastructure such as roads, the responsibility of maintaining and ensuring accountability of it lies with the government. In the current scenario, the burden of providing this infrastructure lies on the private sector and with data trustees as proxies for ensuring accountability**. While the infrastructure regulation and governance in traditional sectors have transitioned from a purely public to public-private partnership model, our experience

[28] https://www.eitdigital.eu/newsroom/news/article/new-report-on-european-digital-infrastructure-and-data-sovereignty/

[29] Economists consider data as an 'experience good' — in other words, its value is unknown until it has been used for a particular purpose. When used for a different purpose, its value may not be the same, in particular because the real value of data does not come from a single dataset, but from combining datasets from different sources. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64954

[30] Dr Michael Mandel, *The Economic Impact of Data: Why Data Is Not Like Oil.* Progressive Policy Institute. 2017.

with such model leaves much to be desired, as interests of people are ignored or overlooked. Transposing such model in data governance, wherein government and large corporates will be in a position to extract value from data without necessarily taking into account concerns of small start-ups and citizens, poses similar risks.

7.11 Another key risk that may emerge from consideration of NPD as public good is possibility of profiling and exclusion errors. If the public interest purpose leads to creation of chargeable benefits or serves interest of only specific communities may create exclusions for consumers who cannot afford such benefits; who may not be able to access such public benefits due to their limited technical capacity or due to entrenched biasness on the part of the data requester. We have already seen this phenomenon in the case of Aadhar, which has created exclusion due technology only mechanisms for availing benefits, absence of manual override, and 'mission creep' that plagued it.[31] In such cases, lack of transparency, accountability and grievance redress will defeat the basis of prescribing HVD as a public good.

Recommendations

7.12 Keeping in mind this jurisprudence, no fixed definition can be prescribed to 'public interest'; however, it should be interpreted in the context that it occurs and should be justified in cases where it can serve a larger benefit to society. This leads to an inherent vagueness for justifying data sharing on the basis of 'public interest'. It is important to weigh the "necessity" and "proportionality" of sharing data *vis-a-vis* externalities created from mandatorily sharing data (anti-competitive effects, hampering commercial interest), to enable which **risk assessment factors and guidelines for 'responsible use of data'[32] on behalf of the data requestors should be stipulated.**

7.13 It may also be noted that in a report by the High Level Committee on Business to Government Sharing in the EU, it was highlighted that it is difficult to define 'public interest' and a one size fits all approach should be avoided. Instead, it indicates towards adopting it as 'a concept' borrowing from the policy of 'services of general interest', which states that *"they are services that public authorities of the Member States at national, regional or local level classify as being of general interest and, therefore, subject to specific public-service obligations*."[33]

7.14 In this regard, we could be informed by the approach taken by Australia in its **Data Sharing and Release Legislative Reforms, 2019. The proposed reform act prescribed**

[31] https://indianexpress.com/article/opinion/columns/excluded-by-aadhaar-4689083/

[32] Katarzyna Śledziewska and Renata Włoch, "Should We Treat Big Data as a Public Good?," in *The Responsibilities of Online Service Providers*, ed. Mariarosaria Taddeo and Luciano Floridi, vol. 31, Law, Governance and Technology Series (Cham: Springer International Publishing, 2017), 263–73, doi:10.1007/978-3-319-47852-4_14.

[33] High Level Committee Report on B2G Sharing - https://www.euractiv.com/wp-content/uploads/sites/2/2020/02/B2GDataSharingExpertGroupReport-1.pdf

a purpose test - the sharing is reasonable and necessary to inform government policy, program and service delivery or for research and development. It further stipulates that the government policy and programs and research should result in outcomes for the entire society and in the case of government service delivery, it should support better outcomes targeted at individuals.[34] (also see Annexure II)

7.15 Moreover, the report recognises that priority HVD domains should be recognised eventually, however; it is necessary to identify these domains before the implementation of the proposed NPD legislation for targeted usage of data based on necessity. Moreover, these domains should be streamlined with targets of National AI strategy, industrial and agricultural policies to create better synergies.

7.16 The report also cites the economic survey of India, to build on the statement of 'data of the people, by the people and for the people'. However, the economic survey had highlighted the need for harnessing data available with the government for the public good rather than obligating the private sector to mandatorily share data.[35] **In this context, the evaluation of the status of open data policies and the trends on usage of such data, gaps and challenges to guide future policy decisions pertaining to target sectors for data use should be undertaken.**

7.17 Thus, it is imperative that the committee goes back to the drawing board and assess, rationale and cost of data sharing, as one size fits all regulatory approach (mandatory sharing) for all kinds of 'public interest purposes' may hamper innovation rather than promoting it.[36] **This is important as many data custodians may not be willing to share the data unless the 'moral necessity'[37] of sharing the data is adequately established by the data trustee. This could only be materialised through better evidence gathering to map the existing data usages, industry readiness, data gaps in the Indian context through undertaking cost-benefit analysis.**

7.18 **Furthermore, it is also important to devise an audit mechanism or requirements of submission of utilization plan for data before making the HVD available. Some such mechanisms have also been prescribed by other jurisdictions such as the UK, Australia and Netherlands. This will be helpful in maintaining accountability as well as assessing related costs and benefits. (also see Annexure II)**

Data Trustees

Issues

[34] https://www.datacommissioner.gov.au/sites/default/files/2019-09/Data%20Sharing%20and%20Release%20Legislative%20Reforms%20Discussion%20Paper%20-%20Accessibility.pdf

[35] https://www.indiabudget.gov.in/budget2019-20/economicsurvey/doc/vol1chapter/echap04_vol1.pdf

[36] https://datalandscape.eu/sites/default/files/report/Story_1_New_format.pdf

[37] Taylor L. 2016, The ethics of big data as a public good: which public? Whose good? Phil. Trans. R. Soc. A 374: 20160126. http://dx.doi.org/10.1098/rsta.2016.0126

7.19 While the committee states that data trustees will be organically created through the coming together of community members, under Section 8, it negates the traditional challenges with the trusteeship framework. It has been observed that the Indian digital economy space is relying on setting up intermediaries to liaison between the end-users and the service providers. For example, iSPIRIT[38] and setting up of account aggregators or the proposal to establish consent managers. **The proposal of these mechanisms at the outset seems novel, however, we should be mindful of the 'intermediary problem' in India. There exists a belief of mistrust in intermediaries, due to their tendency of tilting towards commercially beneficial interest leaving the actual intended beneficiaries behind.**

7.20 These observations of the **'intermediary problem' were reflected in the report of Vijay Kelkar with reference to public-private partnerships (PPP). The report stated that there is a need for improvement in the existing PPP models as they should not be seen as a tool for the government to evade its responsibilities to ensure service delivery to the citizen.** Overall, the report recommended that there should be better risk allocations with benefits to the citizen at the core.[39] In the context of the NPD framework, the report prescribes for data trustees to have a 'duty of care' to the community. **However, the mechanisms for the application of 'duty of care' and safeguards to ensure that data trustee does not become a tool for the government to evade accountability are missing**.

7.21 Furthermore, data trustees may itself create competitive disadvantages for data custodians, if they also have similar mission statements and objective. For example, National Payments Corporation of India, which is a Section 8 company and maybe eligible to be a data trustee, at the same time, may also hold competitive interest in case of processing requests related to fintech sector. This could create further conflicts and new form of data monopolies. Thus, in an attempt to solve one vice, the report may create a bigger vice, albeit unintentionally.

7.22 **Another key factor that is missing from the report is mechanisms to ensure independence and mechanisms of check balances for the data trustee to avoid exploitative conduct.** While the report states that appropriate grievance redress mechanisms would be set-up to address concerns, the mechanism of applicability, or the guidance on the kind of harms that may emerge for the community and consumers are missing. CUTS privacy perception survey highlighted that most consumers are not aware of avenues for grievance and only those who have earlier experienced a privacy breach went on to complain about it.[40] This highlights that without clear prescription and

[38] https://ispirt.in/

[39] https://www.prsindia.org/sites/default/files/parliament_or_policy_pdfs/1451885505_Report%20Summary%20-%20Kelkar%20Committee%20PPP.pdf

[40] https://cuts-ccier.org/pdf/survey_analysis-dataprivacy.pdf,https://cuts-ccier.org/pdf/policy-brief-grievance-redress.pdf

understanding of harms, and approachable avenues for redress, communities or consumers would not be able to indulge in redress mechanism.

Recommendations

7.23 In order to create greater trust among parties in the data ecosystem, the 'duty of care' should flow both ways i.e. for the community as well as data custodians. **There should be a requirement of formulation of precise problem statements for the usage of data, the technical capability of data businesses to share data, the usability of data and trust amongst parties in the data ecosystem.[41] These considerations should formulate the part of 'duty of care'.**

7.24 Another key consideration for achieving greater trust should be to ensure the independence of data trustees, and their ability to represent interest of communities. For this**, the report should specify pre-conditions such as data businesses and data trustees should not dictate data sharing for the purposes that might be in their own beneficial interest, have sustainable funding models such as separate funding from philanthropic donors or acquiring subscriptions from community members so that the drive to make a profit does not override data trust's purpose, and not allowing the requesters to be data trustees to avoid exploitative conduct (i.e. cannot be a judge in your own cause).[42]**

7.25 Furthermore, an appropriate ex-ante risk assessment is necessary to identify collective and individual harms that may emerge from data uses and based on that violations should be prescribed. This would help all the stakeholders in the data sharing chain to understand their responsibility. At the same time, it is also important to find alternative avenues of grievance redress such as through setting up Consumer Service Cells by the data trustees on the lines of CUTS' Grahak Sahayta Kendras,[43] which could act as mediator or conciliator in resolving the complaints.

7.26Moreover**,** data stewardship and data trustees are evolving models of data governance. Countries like the UK have first implemented pilot projects for assessing the challenges and impact of data trust models. **In order to understand the suitability of this governance model in India, pilots should be undertaken in different sectors, as has also been done in the UK.**

[41] https://medium.com/data-stewards-network/the-three-goals-and-five-functions-of-data-stewards-60242449f378
[42] https://docs.google.com/document/d/118RqyUAWP3WIyyCO4iLUT3oOobnYJGibEhspr2v87jg/edit#
[43] Consumer Care Centre (Grahak Sahayta Kendra) | CUTS Centre for Consumer Action, Research & Training (CART)," https://cutscart.org/consumer-care-centre-grahaksahayta-kendra/

8. Non-Personal Data Authority (NPDA) and Regulatory Overlaps

- *NPDA has an enabling and enforcing function.*
- *It will work with industry participation and should be harmonized with other bodies like the Personal Data Protection Authority (DPA), CCI, etc.*

Issues

8.1 The report prescribes for the exclusive jurisdiction of the NPDA on the basis that the objective of the authority is to adjudicate on the rights of the community and provide initial support to the startups and not to address anticompetitive effects. However, this seems to be conflicting with the stated objective of unlocking the economic value of data. **The 'case for regulating data', has an underlying tone of inequitable distribution that exists with respect to data which stipulates the need for regulation for the public interest. It seems that the report has indirectly tried to address the problems of inequitable distribution, market failure and citizen, all of which could be covered under competition law.**

8.2 Also as mentioned before, the committee has at times equated data as a tangible physical resource. This has also prompted the committee to invoke constitutional provisions as well as case precedents related to tangible resources like land, to justify the way the data must be shared, used, and owned. Further, raising issues on the simultaneous overlapping ownership rights and privileges. This assumption is bringing in confusion and overlap of different approaches and regulations when it comes to deriving the value of data.

8.3 The report states that the copyright protection under the Indian law would not apply to high-value datasets, as no skill or creativity will be required in the compilation of such datasets given that even the 'fields of data' will be predetermined. **However, it should be noted that every dataset may have different levels of originality and creativity and in some cases, the 'fields of data' may also be innovative. This is specifically true in the case aggregated dataset, wherein the 'field of data' is determinant of analysis applied to a particular dataset. This can attach the standard 'modicum of creativity' even with the data fields. This can potentially bring challenges due to contradictory messages and a narrow view taken by the committee on intellectual property rights in data.**

8.4 **Additionally, this will also cause conflict of NPDA's jurisdiction with the Copyright Board.** There can be conflict on determination of copyrights by the board on a certain dataset and maintaining its records and NPDA's obligation and jurisdiction to maintain open data directory of meta-data.

8.5 Although Indian law does not give protection to trade secrets, **India is a signatory to the TRIPS agreement and is obligated to protect the secrecy of commercially valuable**

information, under Article 39. While the report identifies that certain raw NPD may be covered under trade secrets, the onus of establishing such coverage is on the data custodians. The report also states that even if trade secrets provisions are applied, they may be overridden through claims of 'eminent domain'. **At the same time, the committee itself notes that we should be cautious in applying such principles in the context of NPD. This creates confusion and leaves the scope for application of eminent domain, which goes against the community rights concept and fall in the realm of property rights.**

8.6 The report states that there is no applicability of the Competition Act in the context of the current framework. Here, the report misses on considering that the Competition Commission of India (CCI), may also have the power to prescribe data sharing for public economic benefits under the essential facilities doctrine. Additionally, the report prescribes for the expropriation of data for economic benefits such as starting of new businesses and developing new value-added services with an underlying objective of equitable distribution due to accumulation of data by Big Tech companies. This seems to be an issue which should come under the purview of CCI. In this regard, the committee has taken a narrow view and negated the overlaps with competition laws and other sectoral regulations in India. **The committee must re-evaluate this narrow view and give proper credit to the CCI, without infringing on its jurisdiction or diminishing its role as a key regulator.**

8.7 Additionally, apart from the horizontal overlap in regulation, there may also be overlaps at the state and centre level. Many of the states such as Karnataka[44] and Telangana[45] have introduced their open data and data sharing policies. Thus, sectors that come under concurrent list of the constitution of India, may create conflicting interests and overlaps.

8.8 Furthermore, the report suggests that consultation should be undertaken amongst regulators; however a specific mechanism for ensuring fruitful consultation is missing. Additionally, **even if a separate authority is to be set-up, due consideration needs to be given to its constitution and independence to avoid violation of the principle of natural justice i.e. "*nemo debet esse judex in propria causa*". Since, the government can take the role of a data trustee, data custodian or data requester, there could be possibility of bias and overreach by the regulator.**

Interface with international data policies

8.9 Another important perspective that the report seems to be missing is its interface with global data policies and its eventual effect on cross-border data flows of India and consequent impact on India's economic growth. The report emphasises on asserting data

[44]https://karunadu.karnataka.gov.in/jnanaayoga/Other%20Reports/KJA%20Bigdata%20Recommendation%20Report.pdf
[45] https://www.telangana.gov.in/PDFDocuments/Telangana-Open-Data-Policy-2016.pdf

sovereignty of India, through regulation. However, even though other jurisdictions, have also included the aim of achieving digital sovereignty, this aim must be put in context with local industrial situations. The Indian Information Technology Industry is highly dependent on data flows, import of digital services etc, and has transformed into a world leading industry in the absence of stringent regulatory framework. This is also evidenced from study conducted by CUTS on economic impacts of data localisation.[46] **Thus, if a balance between ensuring cross -border exchange of digital services and data and promoting innovation and the indigenous level is not ensured, it may dis-incentivise investments and impact the burgeoning start-up ecosystem. Apart from this, non-standardisation of anonymisation techniques will also bring further privacy and compliance burden within cross–border data flows.**

Recommendation

8.10 Broadly, the committee should be urged to take a broader and more progressive view when it comes to jurisdictions and the applicability of different laws and policy in the context of NPD. Avoiding umbrella regulations and leaving no room for sectoral regulations on data sharing would be the first step to avoid the kinds of regulatory overlaps that might make it complicated to simplify in the future**.**

8.11 Thus, **instead of increasing the compliance and regulatory burden on the industry the problem of market imbalances, ensuring citizen welfare and equitable distribution of resources can be governed by the Competition Commission of India (CCI). Similarly, the privacy concerns should be handled by the proposed DPA under the PDP Bill.** We have also emphasized this in our comments on the previous version of the report (please see Annexure III). **While it is true that there are concerns regarding the capacity of the CCI, instead of creating new regulators, the focus should be on increasing capacities of the existing ones.** Other jurisdictions such as the EU and United States have both taken this approach and have strengthened their competition tools to address concerns regarding inequitable distribution of data.

8.12 In addition, a collaborative approach is required to deal with regulatory overlaps. Economic regulators have long used this model, the UK being the primary example**. An authority comprising of all the concerned bodies and regulators (in this case the DPA, CCI and sector regulators) can be formed to decide and adjudicate on the separation and limitation of each of their jurisdictions. This authority can also be empowered to resolve matters which cannot fall under any one of the regulations.**[47] Memorandum of Understandings (MOUs) is another tool for such regulatory collaboration.

[46] https://cuts-ccier.org/pdf/data-localisation-indias-double-edged-sword.pdf

[47] Collaboration between Economic Regulators: Options for embedding joint working between economic regulators - government response to the consultation (publishing.service.gov.uk)

8.13 Considering that the need for setting up a regulatory body such as NPDA arises in future, ensuring independence of the authority should be paramount. **For this, a selection committee including representatives from the industry, civil society and experts should be formulated. This will ensure that the authority would function without undue pressure from governments.**[48]

8.14 The committee must also take a liberal and settled view in the global context on how to treat data, and what kind of rights, and responsibilities are to be associated with it. Given the fact that several other jurisdictions are defining public data, it's likely that international trade agreements will come with a caveat of liberal use and view of data in the future. **The committee must therefore ensure that the framework is aligned with other policies that the government is pushing for, such as foreign trade policy to ensure greater convergence.**

[48] http://www.cuts-ccier.org/pdf/CUTS_Comments_on_the_draft_Regulatory_Reform_Bill-2013.pdf

9. Data Sharing Purpose and Mechanisms

- *Sovereign purpose - the NPDA will not have the authority over such adjudication.*
- *Public good purpose – sharing of HVD for a public good purpose*
- *Business purpose – The report states that such data sharing already exists, and no recommendations are made for this.*
- *The committee has prescribed a process of sharing, wherein, the data trustee will make a request to multiple data custodians to formulate HVD.*
- *If the data custodian refuses a request, NPDA will adjudicate.*
- *Nominal charges could be charged by the data trustee for fulfilling the request and reasonable charges to be paid to the data custodian for processing (anonymisation, data sharing and aggregation but not collection*)
- *Non-personal data derived from personal data shall inherit the sensitivity of the underlying personal data for storage requirements as specified in the PDP Bill.*

Issues

Data Sharing Purpose

9.1 Overall, while it appears that the committee has ostensibly reduced the scope of the framework to only public interest purpose, however, the **committee has defined the public good purpose with a wide room for interpretations in its current form. As has already been stated in 6.1., there is a broken link between the objective of community benefit and the way it has been defined and approached in the current framework. As a result of the vague and broad ambit of public interest purposes, the businesses involved in the NPD ecosystem would suffer from policy uncertainty, burden of compliance and the stifling of innovation.**

9.2 On the other hand, withdrawing adjudication of **NPDA in cases of data sharing for sovereign purposes, may give unfettered access to the government of both personal and non-personal data without any oversight mechanism.** There already has been much criticism around blanket exemption being given in the PDP Bill for sovereign purposes.[49]Without any specification of the constitution of sovereign purposes; exemptions under the PDP Bill; along with lack of oversight under this framework, will give unaccounted access to data without legal checks and balances**. This will fuel risks of surveillance, thereby threatening free speech.[50] The report has also missed on looking at this from a global perspective, which poses a risk for India to not be included in data security and data flow agreements due to lack of checks and balances and judicial oversights on sovereign purposes**.

[49] https://cuts-ccier.org/pdf/policy-brief-exemptions-for-the-state.pdf
[50] https://cuts-ccier.org/pdf/submission-pdpb-2019.pdf

9.3 Additionally, while the committee states that private sharing is already happening in the current ecosystem and does not require any adjudication**, it should be mindful of the effect of the broad ambit of public on private sector sharing. If the data requestor would perceive a certain dataset would be extracted as an HVD, without any transfer of incentive, there would be no motivation to indulge in private sector sharing**. This detriment would in-turn demotivate data custodians to indulge in activities such as data collaboration or pursuing data markets.

Recommendations

9.4 **When determining the data sharing for sovereign purposes, it is vital that the committee recognises the importance and applicability of the three-pronged test of proportionality, legality, and necessity which the Supreme Court of India has interpreted in the case of *Justice KS Puttaswamy v. Union of India*.[51] Similar conditions have also been prescribed in other jurisdictions EU, UK, Netherlands and Australia; wherein data is to be prescribed for law enforcement purposes.** (please also see Annexure II)

9.5 Additionally, the determination of the purpose of sharing should emerge from necessity and reasonableness. To assess such needs, there is a need for further assessment on a sectoral basis to determine the gaps and issues and identify synergies between trade, industrial and agricultural policies, through undertaking cost-benefit analysis. A similar approach has been taken by the UK in its proposed National Data Strategy. Data Sharing Mechanism - Mandatory Data Sharing and Incentive Structure. (also see Annexure II)

Mandatory Data Sharing and Incentive Structure

Issues

9.6 The overall mechanism at the outset seems to be coherent and streamlined, however, the devil lies in the detail. The committee prescribes mandatory data sharing with only caveat of NPDA adjudication, posing risks of disincentivisation. An OECD assessment conducted on the risks of data sharing, pointed out that while regulation may impose data access, it may also undermine incentives to invest in data in the first place, in particular when data commercialization and licensing are not viable options. For instance, for organizations, particularly start-ups, which build their competitive advantage based on data **lock-in, mandatory data access and sharing could undermine their ability to compete, to a point where their incentives to invest in data collection may be too low to enter a particular market. For some start-ups, this could mean that they lose their**

[51] https://theodi.org/article/odi-data-trusts-report/

attractiveness as acquisition targets of larger firms, and thus their economic value. [52]

9.7 Mandatory data sharing along with loose criterion of 'public interest purpose' creates a misalignment of incentives and externalities through the chain of data sharing. This gap needs to be assessed in light of incentive misalignments and externalities that may emerge from mandatory sharing of HVD as 'public good'.

9.8 **The report envisages sharing of HVD for community benefit; however, they may not always be aligned with the interest of the data custodians. While the report provides for 'reasonable charges' to be paid to the data custodian, the collection and storage of data may also involve proprietary knowledge and associated costs.** For example, a new technology of data sensors being utilized for collection of agriculture data would also involve investment and innovative aptitude. However, the report completely negates, determination of incentives around these. Moreover, while these costs could be easily accrued by Big Tech companies, it will pose a burden on smaller players.

9.9 Furthermore, the data businesses may themselves strategize to expand business or provide chargeable public benefits; or the data business maybe in the business of providing data to the government for carrying out its functions. **In such cases 'proportionality' needs to be struck between private costs (current and foreseeable) and public benefits. Overall, it needs to be ensured that the expected public benefits are more than the costs accrued for making the data available.**[53]

9.10 More generally, the responsibility for maintaining other public goods such as water or roads lies with the government; however, the current framework differs in this regard. The transaction cost of creation, identification and fulfillment of the data sharing requests have been transferred to the data trustee (government or non-governmental organization**). However, in a situation where proper and sustainable incentive structures are not specified for data trustees, it may lead them to prioritize private interests over public or community interests.** In this context, the UK, which has done a pilot project of data trustee model has emphasized on the need for ensuring appropriate funding models through which sustainability, as well as the independence of data trustees, could be maintained.[54] (also see Annexure I and II)

9.11 On the side of the data requester, in order to fully realize the public interest potential of data, appropriate data infrastructure, technical capability to ensure the usability of data, and proper network infrastructure is vital. **These present entry level costs for data requestors, which can only be compensated if they make their services chargeable unless there is government funding to cover such costs. This presents a gap between**

[52] "Enhancing Access to and Sharing of Data : Reconciling Risks and Benefits for Data Re-Use across Societies" (OECD, 2019), ./sti-2019-1215-en/index.html.
[53] https://ec.europa.eu/jrc/sites/jrcsh/files/jrc119947.pdf
[54] https://theodi.org/article/odi-data-trusts-report/

intended public benefits and the mechanisms to maintain to realize and sustain that public benefit, through start-ups.

9.12 Furthermore, the report has retained on imposing data localisation requirements for certain NPD, which would further increase compliance burden and investment costs for data businesses along with increasing privacy and security risks.[55] This has been evidenced from the study conducted by CUTS on the economic impact of data localisation, which indicated that localisation requirements could impede India's Information Technology Industry as it would be detrimental to digital service and exports and imports.[56]

Recommendations

9.13 It has been observed that India has a tendency to overregulate without consideration of unintended consequences. Even other jurisdictions which have or are in the process of prescribing data sharing frameworks have taken stock of the industry readiness, trends of data usage and existing policies before prescribing sharing frameworks for their economy before prescribing any framework or regulations. For example, the EU has undertaken extensive impact assessment exercises,[57] UK is in the process of public consultation[58] and Australia has assessments and has relied on the report of its Productivity Commission[59] taking account data usage in the country (see Annexure I). **Thus, cost-benefit analysis to determine the associated costs and incentive structure is vital to understand whether benefits outweigh the costs associated.**

9.14 Even if in due course assessments reach the conclusion that data sharing should be prescribed, it is imperative that we look at alternatives to mandatory sharing which have been adopted by other jurisdictions. For example, **alternative approaches such as contract guidance or data sharing, voluntary frameworks, sectoral level approach, or only prescribing mandatory when markets fail, etc. should be assessed.** Furthermore, even in cases of mandatory sharing incentive mechanisms such as viability gap funding and tax credits for sharing and using of data for public interest and otherwise should also be assessed. For instance, the novel approaches such as 'data altruism' taken by the Data Governance Act of EU.[60] These may present alternatives to mandatory data

[55] https://cuts-ccier.org/pdf/Findings_of_Consumer_Impact_Assessment_of_Data_Localisation.pdf
[56] https://cuts-ccier.org/pdf/data-localisation-indias-double-edged-sword.pdf
[57] https://ec.europa.eu/digital-single-market/en/free-flow-non-personal-data, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066&from=EN, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy#a-single-market-for-data, https://ec.europa.eu/digital-single-market/en/guidance-private-sector-data-sharing
[58] https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy
[59] https://www.pc.gov.au/inquiries/completed/data-access/report
[60] https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-european-data-governance-data-governance-act

sharing with incentives wherein the purpose of the data sharing could be achieved without dis-incentivizing data custodians. (also see Annexure II)

9.15 Moreover, these issues necessitate a clear understanding of who is bearing the cost of every step for providing access to HVD and who is the targeted beneficiary**. While these may be difficult to predict without undertaking an impact assessment, as a safeguard, a utilization plan for the HVD should be submitted with a data request. This approach is also followed by Finland in its Findata initiative to provide access to health data. Data businesses could also be given the right to prescribe reasonable and necessary purpose limitations on the usage of data, in certain circumstances.** (also see Annexure II)

10. Technological Architecture

- *Guiding principles – mechanisms of accessing data in the forms of API, distributed data security, creating standardized data sharing approach, prevent de-anonymisation.*
- *Committee has prescribed three-tiered system architecture.*

Issues

10.1 While the committee's technical guiding principles are in the right direction, there is no clear assessment of the current technical capacities of both the data custodians and the data requester to leverage on this technological architecture. **Apart from technical capacities, the technological architecture might require a business to change their operations or require investment in building more capacities. This will also add to their engineering and technical costs, which would also necessitate assessment of financial capacities.**

10.2 **While the report states that uniform data sharing standards should be adopted, however before this, ensuring appropriate data quality is also vital.** In this regard, an OECD assessment has pointed out that, "*many datasets are not of the requisite quality, are not adequately documented or organised, or are of insufficient (or no) interest for use by others"*. This leads to lack of a common understanding of what quality means in the context of data is a major source of uncertainty among organizations.[61] This observation is also supported by other studies that have pointed out that data analysis can generate promised value only when adequate hardware systems are in place. These issues with quality emanate from prevalent challenges such as - lack of intelligent Big Data sources; the need for scalable real-time analysis capability; lack of support (in networks) for latency-bound applications; the need for necessary augmentation (in network support) for peer-to-peer networks; and rethinking on the cost-effective high-performance storage subsystem. [62]

10.3 **In the Indian context, it is very difficult to determine availability of existing capacities to leverage data sharing infrastructure without taking stock of current shortcoming and data gaps. In this context, the experience of open data sharing in India has shown that available data is usually in a format that is not machine-**

[61] Business Models For Sustainable Research Data Repositories" (OECD, 2017). http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/STP/GSF(2017)1/FINAL&docLanguage=En

[62] Wasim Ahmad Bhat and S.M.K. Quadri, "Big Data Promises Value: Is Hardware Technology Taken Onboard?," ed. Professor Leroy White and Professor Xu Chen Dr Xiaojun Wang, *Industrial Management & Data Systems* 115, no. 9 (January 1, 2015): 1577–95, doi:10.1108/IMDS-04-2015-0160.

readable and usage, rendering the purpose of sharing futile. The committee should be mindful of these shortcomings before prescribing a new technological architecture.[63]

Recommendations

10.4 To address these concerns, the first step should be to assess the current technical capacities of start-ups and determine the gaps and then prescribe a framework that can stimulate the businesses to build capacities. In this regard, we could also be informed by the approach taken by other jurisdictions that have adopted the principles of **findability, accessibility, interoperability and reusability (FAIR) to ensure quality data.**[64] (also see Annexure II). These principles should be the starting point of data standardization and the government should facilitate businesses to achieve these standards. Additionally, we should learn from the experience of open data initiatives and technical concerns in the implementation of National Data Sharing and Accessibility Policy.

For any clarifications/further details, please feel free to contact Amol Kulkarni (amk@cuts.org)/ Shubhangi Heda (sbg@cuts.org)/ Setu Bandh Upadhyay (sbu@cuts.org)

[63] https://www.newindianexpress.com/states/kerala/2020/nov/28/kerala-dilly-dallying-on-open-data-sharing-policy-2228995.html

[64] https://www.government.nl/documents/reports/2019/02/01/dutch-vision-on-data-sharing-between-businesses

ANNEXURE I

Comparison Matrix on Rationale, Assumption and Assessment of Market and Regulatory Failures

Data Sharing Frameworks	Rationale and goals	Assertions behind of rationale	Targeted policy, market and regulatory gaps	Policy Maturity	Market Maturity	Process followed and timelines
Cross-Sectoral and Umbrella frameworks/initiatives/strategies/ guidelines for data sharing						
European Union (EU)						
Framework for the free flow of non-personal data in the European Union 2019[65]	**The objective of the framework is to achieve data mobility, across member states** in Europe which is currently inhibited by data localization practices and mandates of the member states to enhance data economy and competitiveness in the industry. The framework also encourages industry to	The Framework is established on the assertion that the development of data economy in EU is hampered sue to - **imposing technological and legal requirements for storing of data in the geography of specific member states; lack of trust; legal uncertainty**[66] **and other vendor lock-in (cloud service providers)**	The impact assessment reports also revealed that there are problems concerning - inefficiencies in data centre sector, loss of growth and innovation potential, loss of operational efficiency and market distortions which needs to be addressed. **The assessment illustrated the high**	The rules proposed by this **framework were made complimentary to the established provision of the GDPR, through which free movement of data across borders could be facilitated.**	The factsheet prepared for the Framework revealed the current and predicted functioning of data flows and their impact. It noted that lower cost of data services and more flexibility to companies could boost EU GDP by 4 % until 2020. **It also identified, predicted additional revenue in other sectors if the data localization**	**Before introducing the framework impact assessment studies were conducted.**[69] The impact assessment specifically considered different scenarios from no-legislation, soft-legislative intervention to strong legislative intervention and its impact in the context of data flows across jurisdictions on social and environmental

[65] https://ec.europa.eu/digital-single-market/en/free-flow-non-personal-data
[66] The impact assessment identified that there is a perceived existence of data localization requirements by businesses and public sector organizations, which limits there choice of location for data processing
[69] https://ec.europa.eu/digital-single-market/en/news/facilitating-cross-border-data-flow-digital-single-market-study-data-location-restrictions

Data Sharing Frameworks	Rationale and goals	Assertions behind of rationale	Targeted policy, market and regulatory gaps	Policy Maturity	Market Maturity	Process followed and timelines
	come up with self-regulatory codes of conduct for sharing of non-personal data.	**practices. These restrictions were also imposed by private sector through contractual and legal requirements to switch service providers.** **These assertions were supported by the public consultation conducted on building a European Digital Economy, in which 62 % of survey respondents (businesses and organisations) supported to remove data localisation restrictions and 55 % said that legislative action was necessary for doing so.**	**prohibitive costs that were imposed by cloud service providers for SMEs for switching data which was further aggravated due to localization requirements,[67] market economy and legal compliance.**		**restrictions were removed.[68] Thus, indicating the effect on the markets from the existing baseline**.	concerns. The impact assessment were conducted through wide consultation with stakeholders.

[67] http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=46844
[68] http://ec.europa.eu/newsroom/document.cfm?doc_id=47000

Data Sharing Frameworks	Rationale and goals	Assertions behind of rationale	Targeted policy, market and regulatory gaps	Policy Maturity	Market Maturity	Process followed and timelines
European Strategy for Data 2020 [70]	The **measures laid out in this strategy contributes to a comprehensive approach to the data economy to increase the use and demand for data and data-enabled products and services throughout the Digital Single Market**[71] **in Europe.** The strategy is designed to **facilitate access and re-use of data in the economy and society**, while keeping those who generate the data in control. Through this	The strategy emphasises on the economic and public value of data. **At the same time, the strategy interchangeably uses the notion of public interest**[73] **and data as 'public good'**. While assessing this value, the strategy accounts for the currents trends of usage of data in various sectors in the EU such as areas of public interest, IoT, could and quantum computing. Moreover, the strategy basis its assertion on serving the need for individual through	The strategy highlights that there is not enough data available for innovative re-use which is reliant on data holder and user and also the nature of data involved. **The strategies identifies the following key issues based in its consultations and observation - e accumulation of data in the hands of few companies creating market imbalances; data interoperability issues within and across sectors;**[75] **and supply**	The strategy at the outset establishes **that the EU has everything which can lead to development of this initiative - technology know how, implementation of regulation and policies like GDPR, FFD, Database rights, Open Data Directive, Cybersecurity Act.** While introducing this strategy there was parallel guidance issued on private sector data sharing, which specifically notes the	The data market assessment tool which mapped the data economy in EU indicated that currently the **data economy accounts for 2.4 % of EU GDP which is projected to grow to 5.8% in 2025.**[78] **Additionally, this strategy came after the European Digital Single Market policy was initiated in 2014, under which data economy and market assessment and release of periodic review of investments in digital infrastructure,**	This strategy **came about as a result of consultations, studies and assessments which have been ongoing in Europe for a few years now**. The creation of the portfolio on 'A Europe Fit for the Digital Age' was created along with the vision of European Digital Single market being discussed in 2015.

[70] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066&from=EN

[71] A Digital Single Market (DSM) is one in which the free movement of persons, services and capital is ensured and where the individuals and businesses can seamlessly access and engage in online activities under conditions of fair competition, and a high level of consumer and personal data protection, irrespective of their nationality or place of residence. The 2014-2019 Commission had identified the completion of the DSM as one of its 10 political priorities. https://ec.europa.eu/digital-single-market/en/shaping-digital-single-market.

[73] The basis of processing data for public interest has been stipulated in the GDPR. https://edps.europa.eu/sites/edp/files/publication/20-06-16_opinion_data_strategy_en.pdf

[75] https://datalandscape.eu/data-driven-stories/what-limits-data-sharing-europe

[78] https://ec.europa.eu/commission/presscorner/detail/en/fs_20_283

Data Sharing Frameworks	Rationale and goals	Assertions behind of rationale	Targeted policy, market and regulatory gaps	Policy Maturity	Market Maturity	Process followed and timelines
	strategy, EU seeks to empower the businesses and the public sector to make better decisions using data. [72]	creating value for economy and society. **The strategy based its logic on used cases in the EU of data sharing [74] and their contribution to the increasing efficiency and saving labour costs**. Additionally, it also emphasises that the proposed strategy should complement the broader industrial strategy to create a data agile economy.	**and demand side problems with data infrastructures** specifically with cloud providers which needs to be addressed. Additionally, it appropriately identifies - the requirement of developing standards and technical tools for exercising rights of data principals as prescribed in GDPR and the e-privacy legislation; developing cybersecurity framework to ensure security within data value chains to develop trust amongst stakeholders; and to promote digital skills so that professional	outcome of the public consultation indicating that at this stage the horizontal legislation for private sector data sharing is not necessary and the same should be proposed at a later stage.[76] There also has been sector-specific legislation and guidance in place for business to business and government to business data sharing.[77]	**artificial intelligence was undertaken** [79] The models of data sharing as proposed in the strategy are also inspired by the existing member state led initiatives such as Finish and French Data Health Hub.	

[72] https://ec.europa.eu/commission/presscorner/detail/en/fs_20_283
[74] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy#a-single-market-for-data
[76] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0232&from=EN
[77] https://ec.europa.eu/digital-single-market/en/guidance-private-sector-data-sharing
[79] https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53056

Data Sharing Frameworks	Rationale and goals	Assertions behind of rationale	Targeted policy, market and regulatory gaps	Policy Maturity	Market Maturity	Process followed and timelines
			expertise can be built within EU.			
Public Sector Information Directive (PSI) 2019[80] (also called the open data directive)	The objective of this directive **is to make public sector data available for commercial and non-commercial purposes**. The framework establishes an open data sharing mechanism for sharing and re-use of public sector data to all entities and individuals. The Directive's key focus is on the economic aspects of the re-use of information rather than on access to information by citizens.	The premise of the directive is based on the need to update the directive based on technological (emergence of Iot and Big Data) and legal developments (GDPR and consultation of European digital economy and development of Digital Singles Market).[81] **The directive basis its assertion on the value of public data in developing internal market and act as a resource for the development of applications for consumers and legal entities.**	**The impact assessment revealed the following issues in public data sharing - dynamic data sharing through APIs is limited; overcharge on re-use of public data which acts as market barrier for new entrants; data from transport, utilities and data generated from public sector funding was not covered in the previous directive of 2013**; and lock in arrangements between public and private sector which only benefits bigger companies.[83]	This **directive comes as part of the larger EU Digital Single market plan and builds on the existing Directive of 2013 for public data sharing**. The idea being harmonisation of data governance and sharing mechanisms when the EU digital strategy comes into effect. The directive also aims for harmonising its provision with the database directive , GDPR and the on-going consultations on European Digital economy	The directive **has been introduced taking into account the evolving markets due to digital transformation of businesses across sectors and is therefore focused towards economic aspects of data use and re-use**. **The impact assessment noted that the direct economic value of PSI is to increase from a baseline of EUR 52 billion in 2018 to EUR 194 billion in 2030.[85]** This was based on assessing how much value each component of PSI has added or is expected to add which	This directive is a revision of a 2013 directive and a replacement to 2003 directive which covered only specific public institutions. This revision in directive comes at a time when Europe is gearing up for its data strategy. The proposal for the revision of the directive was made as a result of its periodic review, after which impact assessment and consultations were undertaken making the directive updated on the consultation of European Data Economy.

[80] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L1024&from=EN
[81] https://ec.europa.eu/digital-single-market/en/news/impact-assessment-support-study-revision-public-sector-information-directive
[83] https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=51645
[85] https://ec.europa.eu/digital-single-market/en/news/impact-assessment-support-study-revision-public-sector-information-directive

Data Sharing Frameworks	Rationale and goals	Assertions behind of rationale	Targeted policy, market and regulatory gaps	Policy Maturity	Market Maturity	Process followed and timelines
		It also adequately **identifies capacity of public sector to collect, reproduce, produce and disseminate wide range of information in many areas in a machine readable form**at. This would also promote transparency and accountability through feedback received from re-users and end-users on the data. To exploit the potential of public data, the focus is on - **providing real-time access to dynamic data via adequate technical means; increasing supply of public data; and for public undertakings and research organisations to tackle new forms of arrangements for sharing data.**	Consultations further revealed following [84] – non-uniformity of data use and sharing practices amongst member states; there exists variety of licensing conditions which hampers effective re-use; costly redress procedures; possibility of database right being used to restrict access and re-use; misunderstanding on appropriate techniques to be used for pseudonymisation or anonymization processes; and lack of clarity on the meaning of public interest.		includes net effects of research institutions, APIs, para-public bodies, exclusive agreements and charging.	

[84] https://ec.europa.eu/digital-single-market/news-redirect/621219

Data Sharing Frameworks	Rationale and goals	Assertions behind of rationale	Targeted policy, market and regulatory gaps	Policy Maturity	Market Maturity	Process followed and timelines
		The directive encourages member states to ensure the transparency in data sharing and public information and to ensure open access to publicly funded research data at all levels.[82]				
Proposal for a Regulation on European data governance (Data Governance Act) 2020[86]	The proposal aims to **produce the draft of the Data Governance Act[87] which aims to foster the availability of data (both personal and non-personal) for reuse and facilitate trust amongst private sector through trusted data intermediaries through introducing a horizontal governance framework.** For this, the proposed act prescribes re-use of public sector data which	The assertion behind the objectives of the proposed regulation is stemming from the objectives highlighted in National data strategy. The regulation also formulate its basis for facilitating the single market for data ad increasing flexibility, which can only emerge through harmonising and plugging gaps in data sharing practices amongst	**The impact assessment identified three problem brackets i.e., low trust in data sharing, issues around reuse of public sector data and collecting data for common good, technical obstacles to data use.** Within these problem brackets, it was specifically identified that the current practices are leading to consolidation of dominant market actors' power due as data	The proposed regulation flows from the **National Data strategy and the aims to European Digital Singles Market**. Moreover, it takes into account the existing policies such as the open data directive, GDPR and existing sectoral level frameworks and builds from it and ensures harmonisation with them. **Furthermore, in**	The factsheet for the proposed regulation predicts the economic value of data for the market and states that the annual economic value of data sharing will increase upto €7-11 billion by 2028. It also noted that there will be an increase 1.3 trillion increase in productivity through IoT data by 2027 and will also add to societal benefits, for instance in the for saving in the health sector	Consultation on the current proposal was initiated after the adoption of National Data Strategy in February 2020. The consultation involved 219 business organisation and companies of which 43.4 % were SMEs. Along with this, 10 workshops were conducted with expertise from different sectors were conducted to gather issues and problems before setting

[82] https://ec.europa.eu/digital-single-market/en/european-legislation-reuse-public-sector-information
[86] https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-european-data-governance-data-governance-act
[87] https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=71222

Data Sharing Frameworks	Rationale and goals	Assertions behind of rationale	Targeted policy, market and regulatory gaps	Policy Maturity	Market Maturity	Process followed and timelines
	was not permitted earlier with assurance technical capability to ensure data protection, privacy and confidentiality, data altruism, certification and labelling framework for data intermediaries to facilitate trust.	stakeholders and member states. The objectives rely on broader assertion that increase in data re-use and availability will add social and economic value based on the industry report in the EU.[88] **At the same, the impact assessment also asserts that the exchange of data amongst private sector from diverse sources to benefit their own value change maybe greater than monetary incentives for data sharing.** **Furthermore, the proposed regulation also aims for facilitating the regional and local level data sharing amongst member states**	intermediation is being provided by dominant forms are non-EU, lack of competing offers leading to increase in transaction costs **which may act as burden for the SMEs. Additionally, it emphasises that limited availability of data will affect Ai innovation and stagnation of data professional and companies. Moreover, within the problem statement it specifically recognises that internal markets are not fully developed enough to achieve economies of scale which results in dependencies on third countries.**	**setting up of governance body it also relies on GDPR kind of data protection board**.	amounting to 120 billion euros.	up horizontal data governance framework.

[88] https://www.vodafone.com/content/dam/vodcom/files/public-policy/Realising_the_potential_of_IoT_data_report_for_Vodafone.pdf

Data Sharing Frameworks	Rationale and goals	Assertions behind of rationale	Targeted policy, market and regulatory gaps	Policy Maturity	Market Maturity	Process followed and timelines
		and businesses so that they can formulate holistic consumer insights and have an alternate business model from the big-tech. Moreover, the assertion bring in the view that since the public sector data has been generated at the expenses of the public and must be fully utilise for the benefit of the society.				
Netherlands						
Dutch Vision on Data Sharing Between Businesses 2019[89] (Under Dutch Digitalisation Strategy)[90]	The strategy aims to facilitate data sharing between businesses where market failed to do so and is unable to organise data sharing or their abuse of dominance by few players in the market. The strategy recognises that the government can	The strategy recognises that data is a resource for the 21st century and its re-use and sharing will benefit business. As a part of the bigger Dutch Digitalisation Strategy to get the Netherlands ready for the digital future, the report deals with the data	Based on the consultations reasons as to why and in what capacity government - intervention would be required- unwilling to share (competitive advantage), being unable to share due to lack of technical standards, not	The strategy recognises the data market growth and the important developments in data regime by the EU like GDPR, by initiatives like iSHARE, and by non-profit tools like My Data Done Right.	Dutch businesses and public authorities have invested significant amount in ICT capital (EUR 26 billion out of a total of EUR 136 billion invested by the Netherlands in 2015) with the view that data will be an important resource. The strategy	The strategy discusses several case studies on different approaches towards data sharing. Based on these approaches, the strategy fills the gap between them. The strategy if somewhat flexible as it hasn't been converted

[89] https://www.government.nl/documents/reports/2019/02/01/dutch-vision-on-data-sharing-between-businesses
[90] https://www.government.nl/documents/reports/2018/06/01/dutch-digitalisation-strategy

Data Sharing Frameworks	Rationale and goals	Assertions behind of rationale	Targeted policy, market and regulatory gaps	Policy Maturity	Market Maturity	Process followed and timelines
	play a role in this if the markets itself have failed to do so and to reduce the risk of privacy breaches and ensuring cybersecurity in data sharing. Additionally, the strategy is inspired by the analysis of the used cases of data sharing in the Netherlands following different arrangements and principles.	sharing processes and frameworks between businesses.	being permitted to share due to legal obligations. The strategy covers data sharing for innovation and increasing competition. It also recognizes that compulsory data sharing maybe introduced for sharing of data for public interest such as competition, freedom of choice, innovation, good health or free-flowing traffic and green economy.	The strategy takes these developments into account before building up a progressive data sharing regime on these developments, ensuring a harmony and market inclusion with existing policies.	realises it's role to encourage data sharing in the growing market and to ensure that the market organises productive data sharing itself, or if dominant providers or platforms that have unique access to certain data are unwilling to share it with other parties. The strategy also talks about its role in limiting risk in areas such as privacy and cybersecurity	into a law or regulation yet.
Singapore						
Trusted Data Sharing Framework[91]	The Framework is **aimed to provide guidance on key considerations to enable data sharing** (such as valuation mechanism for data, structuring legal relationships to enable	The framework states that **data forms a valuable asset for developing Artificial Intelligence (AI) and companies and will add 5-6 % on their outputs**.	The framework notes that based on industry feedback, the data-sharing ecosystem is still in a nascent stage and guidance is still very much required to help organisations, including professional data service	**The framework comes at a time when Singapore already has a robust data law like the Personal Data Protection Act 2012.** Infact, consultations were undertaken on improving the	**It draws from the use cases of data sharing such as bilateral information sharing between banks and telcos to increase customer service and experience; information sharing**	The framework is reliant on external studies and cites the Personal Data Protection Act 2012 for a majority of its approaches. In 2020, the PDPA Act was amended to ensure

[91] https://www.imda.gov.sg/-/media/Imda/Files/Programme/AI-Data-Innovation/Trusted-Data-Sharing-Framework.pdf

Data Sharing Frameworks	Rationale and goals	Assertions behind of rationale	Targeted policy, market and regulatory gaps	Policy Maturity	Market Maturity	Process followed and timelines
	data sharing, technical amongst private sector to address trust security concerns considerations, consent mechanism and other operational considerations) . **This Framework is just a guide for industry and not for compliance**	The objective of the framework **also supports Singapore's Digital Economy Framework for Action, which emphasises on developing infrastructures to build capacities** specifically in the Infocom and Media for tapping in data flows and AI.[92] Additionally, **the framework recognises that it is difficult for business to value their data, thus along with this framework, guide on valuation of data was also released**.[93]	providers overcome the concerns of data sharing.	framework to balance data sharing and data protection concerns. At the same time, Data Protection Trustmark certification scheme was also introduced. **This framework also came as backdrop of Singapore's intent to participate in APEC Cross- Border Privacy rules system and APEC Privacy Recognition for Processors System**.[94] Moreover, along with the current framework, a guide to data valuation, proposing different approach to a valuation was also introduced. It also fills in for IP and Copyright laws which do not	**between Credit Information Bureau in Singapore and banks**, which gives better information on credit risks, data sharing in real estate sector between property service provider and real estate companies.	ease in data sharing in cases of contractual necessity and legitimate interests.[96]

[92] https://www.imda.gov.sg/-/media/Imda/Files/SG-Digital/SGD-Framework-For-Action.pdf
[93] https://www.imda.gov.sg/-/media/Imda/Files/Programme/Data-Collaborative-Programme/Guide-to-Data-Valuation-for-Data-Sharing.pdf?la=en
[94] https://www.nas.gov.sg/archivesonline/data/pdfdoc/20170727002/Developing%20a%20Trusted%20Data%20Ecosystem%20to%20Support%20Singapores%20Digital%20Economy.pdf
[96] https://fpf.org/2020/11/18/singapores-personal-data-protection-act-shifts-away-from-a-consent-centric-framework/

Data Sharing Frameworks	Rationale and goals	Assertions behind of rationale	Targeted policy, market and regulatory gaps	Policy Maturity	Market Maturity	Process followed and timelines
				address this. [95] Thus, the framework is merely providing guidance to data partnerships in an already existing policy regime		
Australia						
Data Sharing and Release Legislative Reforms, 2019[97]	**It introduces the standards for legislation that will empower government agencies to safely share public sector data with trusted users for specified purposes**. It aims for streamlining and modernising data sharing, overcoming complex legislative barriers and out-dated secrecy provisions. It forms the basis of the new regulation to be introduced for purposes of sharing of such data.	**The Australian government released this framework based on the Productivity Commission's (PC) report which aimed for increasing public sector data availability for better delivery of digital services.** This reform framework also asserts that access to data **will increase citizens' access to information through one contact point; will reduce time and access; and will help in**	The Productivity Commission's report identified the areas and organisation in the public sector where most data is retained and made a comparative assessment with other countries regarding the availability of open data. **In this assessment, it was found that Australia was lagging in data availability resulting from inconsistent practices and no single approach to public sector data sharing.**	Before the current framework, **Australia had an 'Open Government National Action Plan' which it plans to complement with this to increase access to public sector data.[99]** Australia also previously introduced Consumer Data Right to facilitate data flow from the private sector. **The Consumer Data Right (CDR) and the Data Sharing and Release legislation are both part of**	The maturity of the **market for data access was indicated through the responses from the consultation in which research institutions and civil society indicated that access to the public sector data is necessary** and could be an important driver of innovation at this stage.	The reforms have been derived from the Productivity Commission's findings on the use and recommended data reforms to unlock the full potential of public sector data. In 2018, the Office of the National Data Commissioner was established within the Department of the Prime Minister and Cabinet to oversee the reforms to improve data sharing and

[95] https://www.imda.gov.sg/-/media/Imda/Files/About/Media-Releases/2019/Factsheet-on-Trusted-Data-Sharing-Framework.pdf?la=en
[97] https://www.datacommissioner.gov.au/sites/default/files/2019-09/Data%20Sharing%20and%20Release%20Legislative%20Reforms%20Discussion%20Paper%20-%20Accessibility.pdf
[99] https://www.pc.gov.au/inquiries/completed/data-access/data-availability-use-government-response.pdf

Data Sharing Frameworks	Rationale and goals	Assertions behind of rationale	Targeted policy, market and regulatory gaps	Policy Maturity	Market Maturity	Process followed and timelines
		assessing sectors-wise funding priorities Additionally, to inform guidelines on the data release it also identified case studies where data sharing could be implemented and related challenges and applicable laws and frameworks.[98].	PC **also noted that their exits lack of trust by both data custodians and users in existing data access processes and protections creating numerous hurdles to sharing and releasing data are choking the use** and value of Australia's data.	**Australia's efforts to reform data legislation.** While the CDR relates to private sector data, the Data Sharing and Release legislation is focused on government-held data. The current framework has taken consideration of the finding of the **privacy impact assessment conducted in 2019.**		use across the Australian public sector.
Japan						
Contract Guidance on Utilization of AI and Data by Ministry of Economy Trade and Industry 2018[100]	These guidelines aims to give standards and details that should be included in be **formulating terms while contracting for data sharing**.	The guidance is based on the assertion that IoT and AI data use is expected to create new value-added and solve societal issues through data collaboration that transcends business boundaries. It is often difficult, however, for	**A survey conducted by a think tank on this issue of data sharing revealed that 15.2 % of companies out of the 562 responses believed that data utilization contracts helped them achieve efficient and reduced costs**, however,	The guidance intends to aid the overall strategy of the Japanese government intended to promote data sharing and innovation. Based on this, **the government had formulated a study group focusing on the**	**It must also be noted that this guidance has also been based on the finding of IoT Acceleration consortium which analysed and provided guidance on used cases of data utilization for IoTs.**[103] Thus, it	The first version of the contract guidance was created **in 2017; however, after receiving comments from industry and associations, a revised version was published in 2018**, on the recommendation of the

[98] https://www.pc.gov.au/inquiries/completed/data-access/report/data-access.pdf
[100] https://www.meti.go.jp/english/press/2018/0615_002.html, https://www.meti.go.jp/press/2019/04/20190404001/20190404001-1.pdf.
[103] https://www.meti.go.jp/english/policy/mono_info_service/information_economy/index.html#two

Data Sharing Frameworks	Rationale and goals	Assertions behind of rationale	Targeted policy, market and regulatory gaps	Policy Maturity	Market Maturity	Process followed and timelines
		businesses to conclude contracts related to the utilization of data or AI technology **due to lack of sufficient experience in contract practices and the gaps in understanding between the parties involved.**	the contracts signed in for this played a significant role in a smooth transaction. **At the same time, 15% of cases also highlighted problems related to leakage of trade secrets and unauthorised use of data utilization.**[101]	**fourth industrial revolution and intellectual property systems. The report of the study group has informed the provisions of this guidance.** **Previous policies related to this guidance involved the establishment of the Personal Information Protection Commission.**[102]	indicated towards the data usage practices followed by the stakeholders.	committee under Professor Toshiya Watanabe.
Act on Special Measures for Productivity Improvement, 2018[104]	The **act is aimed at attracting investment and facing international competition through increase productivity in the IoT, big data** and artificial intelligence. Notably, the provision under this act are subject	This act had been enacted at the backdrop of **Japan's 'Economic Policy Package of 2017', to address the disruptive changes and international competition which is generated by emerging technologies. The act will help gain**	The **Economic Policy Package of 2017 recognized that Japan had been facing sluggish growth in sectors such as automated driving, health sector, agriculture, construction and financial sector.** For this within the policy, Japan	As a support to the New Economic Policy Package 2017, the act ensures that the regulations do not lag behind the planned objectives of the policy package.	The act establishes a "regulatory sandbox" and provides tax breaks to encourage IoT investment for facilitating data sharing, and to encourage SMEs to invest in business facilities, in turn driving the market growth.	The act was drafted based on consultations under the cabinet office and was introduced in June 2018.

[101] http://www.hitachi.com/rev/archive/2019/r2019_03/pdf/P057-063_R3a03.pdf
[102] https://www.ppc.go.jp/en/
[104] https://www.meti.go.jp/english/press/2018_06/0606_001_00.html

Data Sharing Frameworks	Rationale and goals	Assertions behind of rationale	Targeted policy, market and regulatory gaps	Policy Maturity	Market Maturity	Process followed and timelines
	to the Basic Act on the Advancement of Public and Private Sector Data Utilization[105] and Act on the Protection of Personal Information	**investment and increase market productivity**. In an OECD assessment, on markets in Japan, it was noted that the government will enhance the development of **smart infrastructures trying to achieve priority vision of government for data-driven society 5.0.** This act was enacted as one such initiative towards building a data-driven economy.	has laid down its target for achieving goals for Society 5.0, with investment in IoT and AI to facilitate growth in the above sectors.[106] For achieving these targets, the proposed act aims for businesses to increase and incentivising data sharing.			
United Kingdom (UK)						
National Data Strategy 2020 (Under Consultation)[107]	This strategy is an all-encompassing data strategy that aims to leverage existing strengths of UK to boost better use of data across businesses, government,	This strategy comes at the backdrop of used cases of data sharing by private companies and various sectors, inspiring the parameters and focus of this strategy.	Before the introduction of the strategy, consultations were conducted which recognised following barriers **for the data economy - lack of**	The strategy acts as an enabler to the **UK AI Sector Deal discussed next and builds on the existing frameworks such as the Research Powers of the Digital**	The UK data market is largest in Europe, with high investments in tech, the strategy therefore seeks to capitalise and prepare for the future markets.	Before the strategy was introduced evidence collection and roundtable consultations were undertaken by the Department of Digital Culture, Media and

[105] http://www.japaneselawtranslation.go.jp/law/detail/?id=2975&vm=02&re=
[106] https://www5.cao.go.jp/keizai1/package/20171208_package_en.pdf
[107] https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy

Data Sharing Frameworks	Rationale and goals	Assertions behind of rationale	Targeted policy, market and regulatory gaps	Policy Maturity	Market Maturity	Process followed and timelines
	civil society and individuals. The strategy focuses on using data to deliver new and innovative services, promote stronger competition, and better prices and choice for consumers and small businesses.	Moreover, the strategy also notes that government has considerably invested in research and partnered with organisations with expertise in the field to develop and test models of data sharing. The strategy also notes from its consultations that - there is an interconnected ecosystem of data including the users and those affected by the ecosystem; there are many component parts to the 'how' of using data, but there is not yet an established consensus on best practice, **views vary markedly on a range of broader questions based on different perspectives** – for	**governance and senior leadership buy-in on data issues; a lack of agreed standards and poor data quality impacting the effective use and interoperability of data; a data skills gap, both specialist and baseline** in the workforce; a fear of privacy issues and negative thinking leading to datasets being 'closed by default'; lack of clarity on data access rights; legacy infrastructure and software; a culture of 'working in silos' with data across both the public and private sectors.[109] It is also intending to fill in the gaps left by the Data Protection Act 2018 which focused on	**Economy Act (2017), which has already enabled the data usage in various sectors for research purposes.** Moreover, the strategy relies on the findings of the Competition Market Authority (**CMA)'s report on online platforms and digital advertising, which highlights that the limited access to data by some companies comparing to tech giants which may limit innovations**.	The **strategy notes that the data economy grew about twice as quickly as the rest of the economy during the 2010, making up about 4% of UK GDP in 2020.** Further, as per the estimates noted by the **report in 2018 the UK exported £190 billion in digitally delivered services (67% of total UK services exports) and imported £90 billion digitally delivered services (52% of UK services imports**). This estimated indicate towards the maturity and the predicted growth of data economy of the UK The strategy aims for businesses to embrace	Sports. The summary findings are available in public domain. The questions for call for evidence were on the themes of people, government and economy. 105 responses were received from various organisation and sectors including ICT, education organisations, businesses, public sector, etc. Through this exercise existing good practices of data access and sharing were also identified. [111] Currently, the strategy is open for public consultation and is proposed to get views of the stakeholder on kind of government intervention that might be apt.

[109] https://www.gov.uk/government/publications/uk-national-data-strategy/call-for-evidence-and-roundtable-engagement-summaries#national-data-strategy-roundtable-engagement-summary
[111] https://www.gov.uk/government/publications/uk-national-data-strategy/call-for-evidence-and-roundtable-engagement-summaries#national-data-strategy-call-for-evidence-summary

Data Sharing Frameworks	Rationale and goals	Assertions behind of rationale	Targeted policy, market and regulatory gaps	Policy Maturity	Market Maturity	Process followed and timelines
		example, on legislation, burdens on business, burdens on the public, privacy and trust, the roles of players in the ecosystem for setting standards etc., **and there is unlikely to be 'right' answer on these questions, or their solutions**, The **trade-offs between objectives will be inevitable** – for example, the benefits of making data open and the costs of maintaining it, **there is wide disparity in engagement with issues around data across the economy and society**.[108] The strategy also identifies that opening up of every dataset may not be the solution. In this context it states that it	personal data similar to the EU GDPR.[110]		technology, leading to job creation by data use, opening up whole new markets and drives demand for a highly skilled workforce.	

[108] https://www.gov.uk/government/publications/uk-national-data-strategy/call-for-evidence-and-roundtable-engagement-summaries#national-data-strategy-roundtable-engagement-summary
[110] https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Data Sharing Frameworks	Rationale and goals	Assertions behind of rationale	Targeted policy, market and regulatory gaps	Policy Maturity	Market Maturity	Process followed and timelines
		will also be important to consider various costs and to ensure that data access is wide enough to reach all the sectors to maximise it value adequately.				
UK AI Sector Deal 2018-19 (Data Sharing Infrastructure)[112]	This 'Sector Deal' sets out actions to promote the adoption and use of AI in the UK and **deliver on the recommendations of the independent AI review- 'Growing the AI industry in the UK'. The strategy proposed for setting up of data trust to tap on datasets help by public and private sector**. In this regard, the deal also forms interlinkages with the goals of UK's industrial and digital	The UK is home to some of the biggest names in AI innovation and training AIs need a vast amount of data, skilled employees, and innovation enablers like testing availability. The deal is intended to benefit the economy and the society by attracting investment, creating jobs, and reaping AI's benefits, all at once. The independent **AI review also accounts the findings of Royal**	The sector deal sets out actions to promote the adoption and use of AI in the UK and delivers on the recommendations of the independent AI review.[113] The review highlighted that there is lack of know-how to proceed in formulating agreements and establish trust between parties and manage the data sharing practice. **Furthermore, apart from building trusts it points at times procedural and legal**	The AI Sector Deal proposed for a data trust model for un-tapping the datasets from both public and private sectors. In terms of existing policies and practices regarding access to data, UK was ranked first in the world on Government performance on open data. The independent AI review which led to this strategy was also contextualised with parallel reports on data	The studies conducted and the report which the deal is based on has talked about approaching maturity of the UK data market. High investment with 33% of European investments captured by the UK, are to be combined with progressive and supportive policies for market growth. The review had estimated that AI could add an additional USD $814 billion (£630bn) to the UK economy by	Studies and several projects were taken into account in preparation of this Deal. Based on the multi-fold recommendations of the 2017 independent report on 'Growing the artificial intelligence industry in the UK', stakeholders from academia, market players, and authorities were contributory to the deal. It was presented in 2018 and finalised in 2019.

[112] https://www.gov.uk/government/publications/artificial-intelligence-sector-deal/ai-sector-deal
[113] https://www.gov.uk/government/publications/growing-the-artificial-intelligence-industry-in-the-uk

Data Sharing Frameworks	Rationale and goals	Assertions behind of rationale	Targeted policy, market and regulatory gaps	Policy Maturity	Market Maturity	Process followed and timelines
	strategy within data economy	**Society's Machine Learning which indicated that large datasets would be needed to improve the outcomes of AI.** Furthermore, the review notes that some of sectors have generate such amounts of data that it could only be processed by AI. For achieving these goals, the deal focuses on enhancing UKs existing data infrastructures considering the use cases of open data and data sharing such as CityMapper, focus on sharing geospatial data.	**costs of data access, which may hinder such access for smaller companie**s.	management addressing ethical (trust and accountability) and governance questions specifically concepts of data stewards and data trusts.[114] Additionally, the review notes that there are existing best practices and data sharing frameworks amongst individual companies which can inform in building trusted data sharing frameworks.	2035, increasing the annual growth rate from 2.5% to 3.9%. Additionally, the market maturity of the AI sector was also contextualised through Industrial Digitalisation Review, which covered the benefits of deploying robotics and AI to improve industrial processes indicating that potential of data infrastructures to add value.	
Sectoral Frameworks/ Initiatives/ Strategies of Data Sharing						
Finland						
Act on the Secondary Use of	The objective of this act is to facilitate effective	The new Act codifies the relevant legislation and	The act is intended to remove the fragmentation	The act was complemented by the	The eHealth strategy observes that that there	The Act requires compliance with GDPR

[114] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/652097/Growing_the_artificial_intelligence_industry_in_the_UK.pdf

Data Sharing Frameworks	Rationale and goals	Assertions behind of rationale	Targeted policy, market and regulatory gaps	Policy Maturity	Market Maturity	Process followed and timelines
Health and Social Data, Finland 2019[115] (the Act)	and safe processing and access to the personal social and health data for steering, supervision, research, statistics and development in the health and social sector. A second objective is to guarantee an individual's legitimate expectations as well as their rights and freedoms when processing personal data. The act aims to create a IT ecosystem which both the supplier and consumers of data would access based on licensing terms.	broadens the possibilities to, under certain conditions, utilize and combine for secondary purposes personal data collected in relation to public or private social and health care operations. The rationale being ensuring full compliance with the applicable data protection legislation while processing sensitive social and health care data for secondary purposes, while also facilitating better cooperation between the public sector and the private sphere.	of data sharing regulations and rules which are scattered across different regulations and sectors such as the Patient's Rights Act (1992/785), Act on Electronic Processing of Social and Health Care Customer Data (2007/159), Bio Bank Act (2012/688) and Medicines Act (1987/395). The Act also aims to address the administrative burden for the secondary users of social and health care data and parallel and slow licence procedures with various authorities.[116]	Health Sector Growth Strategy for Research and Innovation Activities Roadmap for 2018-18[117] and Information to Support Well-being and Service Renewal: eHealth and eSocial Strategy 2020 (eHealth Strategy). Standards for the contents of electronic medical records have been developed since the 1990s, and technical data transfer standards since the 2000s. Active efforts have been made to standardise the content and technology of information	was a regional development of availability of patient information since mid-2000s in the public sector, however, it was not as widespread in the private sector. [120] Over time, Finland has defined as a priority the development of tools for health professionals, that will enable sharing of distributed patient information securely, leading to innovation in non-profit eHealth and private eHealth providers who work regionally in partnership with the public system.[121]	and was changed significantly during its proposal phase by the parliamentary committees. Since 2011, after a series of policies and public discussions, a national consensus has been reached through multiple strategies and programmes about the importance of knowledge-based decision-making and linking information and knowledge management to digitisation, experimentation, openness and integration of services. A working

[115] https://stm.fi/documents/1271139/1365571/The+Act+on+the+Secondary+Use+of+Health+and+Social+Data/a2bca08c-d067-3e54-45d1-18096de0ed76/The+Act+on+the+Secondary+Use+of+Health+and+Social+Data.pdf
[116] https://blogs.dlapiper.com/privacymatters/finland-parliament-approves-new-act-on-the-secondary-use-of-social-and-health-care-personal-data/#:~:text=The%20Finnish%20Parliament%20has%20approved,effective%20within%20the%20following%20weeks.
[117] https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/75145/MEE_guidelines_8_2016_Health_sector_growth_strategy_17062016_web.pdf
[120] https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/74459/URN_ISBN_978-952-00-3575-4.pdf?sequence=1&isAllowed=y
[121] https://www.tandfonline.com/doi/pdf/10.3402/ijch.v63i4.17749

Data Sharing Frameworks	Rationale and goals	Assertions behind of rationale	Targeted policy, market and regulatory gaps	Policy Maturity	Market Maturity	Process followed and timelines
				management in the social welfare sector since the mid-2000s. Following this, National Kanta Services were formulated consisting of patient data repositories which were also accessible to the citizens.[118] In 2013, The European Health Telematics Association on evaluation of Kanta Services, stated that Finland is a model country for eHealth.[119]		Committee was set up to Formulate the Act. The Act was proposed to the government in 2017, on which expert hearing and debates were conducted resulted in suggestion for amendments in 2018. After which the new Act was proposed and passed in 2019. The Act, therefore, in a series of regulations to transform Finland to significant platform based economy came into force in May 2019, with a steering committee to oversee the beginning of its implementation stage till June 2019.[122]

[118] https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/74459/URN_ISBN_978-952-00-3575-4.pdf?sequence=1&isAllowed=y
[119] https://blogs.dlapiper.com/privacymatters/finland-parliament-approves-new-act-on-the-secondary-use-of-social-and-health-care-personal-data/#:~:text=The%20Finnish%20Parliament%20has%20approved,effective%20within%20the%20following%20weeks.
[122] https://www.sitra.fi/en/publications/a-finnish-model-for-the-secure-and-effective-use-of-data/#abstract

ANNEXURE II

Comparison Matrix on Approaches of Data Sharing

Parameters for Synthesis	Rationale and Goals	Scope of Data Covered and Stakeholders Affected	Purposes of sharing and expectation of value creation	Mechanisms of Governance	Incentives and valuation of data	Checks and Balances
Cross-Sectoral and Umbrella frameworks/initiatives/strategies/ guidelines for data sharing						
European Union (EU)						
Framework for the free flow of non-personal data in the European Union 2019[123]	The objective of the framework is to achieve efficiency in data processing and create 'EU Digital Singles market through increasing data' **mobility across countries which has been inhibited due to data localisation practices of member states such as imposing technological requirements for storing of data in the geography of specific**	**Applies to non-personal data**. In case of mixed data sets, it only applies to non-personal part of datasets and in cases where **personal and non-personal data are intrinsically linked, the General Data Protection Regulation (GDPR) prevails**.	It aims to facilitate the flow of data to competent authorities for official and legal duties as well as amongst private sector organizations and companies for commercial and economic purposes. These purposes are not further elaborated and will be based on self-regulatory codes developed by industry bodies.	The member states are required to update the European Commission about any new data localization framework introduced by them. The commission is responsible for updating the details of the same and making them available publically through a website. The framework encourages the **development of self-regulatory codes by the industry to facilitate**	**Based on self-regulatory code of conduct.** **No valuation mechanisms for data are given.**	The framework prescribes for following conditions for flow of data- porting data in a structural and readable manner, sufficient information to be given to users before porting, certification mechanism to compare quality management, information security and generate awareness about code of conduct The framework specifically states that **any anonymised data that has the possibility of de-**

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

Parameters for Synthesis	Rationale and Goals	Scope of Data Covered and Stakeholders Affected	Purposes of sharing and expectation of value creation	Mechanisms of Governance	Incentives and valuation of data	Checks and Balances
	member states and other vendor lock-in (cloud service providers) practices. **Before introducing the report impact assessment studies were conducted.**[124]			**porting of data based on the principles of transparency ,interoperability and taking due account of open standards.**		**anonymization will be considered as personal data**. The commission has been directed to submit a report on evaluating implementation of this framework by 2022.
European Strategy for Data 2020 [125]	The measures laid out in this paper contributes to a comprehensive approach to the data economy that aims to increase the use of, and demand for, data and data-enabled products and services throughout the Digital Single Market in Europe. The strategy at the outset establishes **that the EU has everything which can lead to**	**Both personal and non-personal data for government to business, business to business, business to government and sharing amongst public authorities are prescribed for.** **For mixed datasets, the strategy notes that business and government should follow practical guidance prescribed for the businesses for mixed**	**The strategy recognizes data sharing for public good and gives examples such as climate change, predicting and coping with natural disasters. However, it does not prescribe for mandatory sharing for such purposes. It also encourages data sharing for economic and commercial purposes.**	Under the strategy **general principle is to facilitate voluntary data sharing**. It stipulated that only where specific circumstances so dictate, access to data should be made compulsory, where appropriate, under fair, transparent, reasonable, proportionate and/or non-discriminatory conditions.	The strategy proposes evaluating existing IPR frameworks with a view to further enhance data access and use (including a possible revision of the Database Directive and a possible clarification of the application of the Trade Secrets Protection Directive as an enabling framework)	The strategy focuses on increasing competence of data principals through empowering them to be in control of their data through tools and means to decide at a granular level about what is done with their data (‘personal data spaces’). For this, it also **proposes to enhance the portability right** for individuals under Article 20 of the GDPR.

[124] file:///C:/Users/Shubhangi/AppData/Local/Temp/ImpactAssessmentSummary.pdf, https://ec.europa.eu/digital-single-market/en/news/facilitating-cross-border-data-flow-digital-single-market-study-data-location-restrictions

[125] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066&from=EN

Parameters for Synthesis	Rationale and Goals	Scope of Data Covered and Stakeholders Affected	Purposes of sharing and expectation of value creation	Mechanisms of Governance	Incentives and valuation of data	Checks and Balances
	development of this initiative - technology know how, implementation of regulation and policies like GDPR, FFD, Open Data Directive , Cybersecurity Act. There also has been sector-specific legislation and frameworks already in place for data sharing. Additionally while introducing this strategy there was parallel guidance issued on private sector data sharing, which specifically notes the outcome of the public consultation which indicated that at this stage the horizontal legislation for private sector data sharing is	**datasets by the earlier directive.**[127] Rights for co-generated data (such as IoT data in industrial settings), typically laid down in private contracts		**Additionally, mandatory sharing is only prescribed when there is a market failure in the particular sector.** **The strategy proposes to explore the need for legislative framework in the form of Data Act of 2021- which would focus on sectoral needs, voluntary data sharing and formulating data pools.**	With regard to valuation of data, private contracts are proposed. Additionally, it states that organisations would voluntarily contribute to data pools in return of data from other organisations, license fee and data analysis tools.	It also proposes to increase data literacy and digital competence amongst the users.

Parameters for Synthesis	Rationale and Goals	Scope of Data Covered and Stakeholders Affected	Purposes of sharing and expectation of value creation	Mechanisms of Governance	Incentives and valuation of data	Checks and Balances
	not necessary and this could be proposed at a later stage.[126]					
Public Sector Information Directive 2019[128]	The objective of this directive is to make public sector data available for commercial and non-commercial purposes. The framework establishes an open data sharing mechanism for sharing of public sector data to all entities and individuals.	**It covers existing documents and research data held by public sector authorities.** The directive does not apply to – Documents on which third parties hold IPR. Documents which have sensitive data pertaining to national security Under the directive, re-use of documents shall be open to all potential actors in the market, even if one or more market actors already exploit added-value products based on those documents. The Directive also introduces the concept of	**Both commercial and non-commercial purposes.**	Request for re-use of the data will be made to public authorities which will take such decision within 20 working days. The public authority will also assess if a license is needed for requested re-use of the data.	Data is made available free of charge. However, the recovery of the marginal costs incurred for the reproduction, provision and dissemination of documents as well as for anonymisation of personal data and measures taken to protect commercially confidential information could be allowed. Member states may exempt bodies for 2 years, where making high-value datasets available free of	The directives prescribes that the re-use of documents shall not be subject to conditions, unless such conditions are objective, proportionate, non-discriminatory and justified on grounds of a public interest objective. When re-use is subject to conditions, those conditions shall not unnecessarily restrict possibilities for re-use and shall not be used to restrict competition

[126] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0232&from=EN
[128] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L1024&from=EN

Parameters for Synthesis	Rationale and Goals	Scope of Data Covered and Stakeholders Affected	Purposes of sharing and expectation of value creation	Mechanisms of Governance	Incentives and valuation of data	Checks and Balances
		"high value datasets", defined as documents the re-use of which is associated with important benefits for the society and economy. The directive indicates to forming separate set of rules ensuring their availability free of charge, in machine readable formats, provided via APIs and where relevant be available as bulk download.			charge by public sector bodies that are required to generate revenue to cover a substantial part of their costs,.	

Parameters for Synthesis	Rationale and Goals	Scope of Data Covered and Stakeholders Affected	Purposes of sharing and expectation of value creation	Mechanisms of Governance	Incentives and valuation of data	Checks and Balances
Proposal for a Regulation on European data governance (Data Governance Act) 2020[129]	The objective is to introduce governance, guidance and standards which could facilitate data re-use and availability.	The **proposed act covers both personal (in an anonymized form deleting commercially confidential information) and non-personal data.** It gives a broader definition of data which covers digital representation of acts, facts or information and any compilation of data in the forms of sound , visual or audio visual recording. In defining, non-personal data it states that it means all other data that is not covered within the definition of personal data in the GDPR. Additionally, it also covers the definition of 'meta-data' which includes date, time and geo-location data, duration activity, connection to other	**The act does not lay down specific purpose for data re-use and availability,** however specifically lays down the condition and standards for re-use. The larger aim of the act is to make diverse data available through various stakeholders in a trusted environment**.**	**The act largely introduces three modes of governance of data sharing and re-uses i.e. - conditions of re-use of public data which is not covered in the PSI directive on the grounds of commercial, statistical confidentiality, protection of IPR and covered by protection under personal data; data sharing through trusted data intermediaries; and data altruism.** For re-use of public sector data, it stated that public sector bodies may impose conditions which are non-discriminatory, proportionate and objectively justified, anonymisation	**The act provides provision for charging fees for the re-use of public sector data**. However, in the case of other data sharing, the act does not prescribe any particular valuation mechanisms.	The act states that in any case the data cannot be used for the purposes other than those specified. Additionally, the regulation gives due consideration to the rights of data holders in the intellectual property regime, **fundamental right of privacy under the GDPR and e-privacy directive and freedom to conduct business.**

[129] https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-european-data-governance-data-governance-act

Parameters for Synthesis	Rationale and Goals	Scope of Data Covered and Stakeholders Affected	Purposes of sharing and expectation of value creation	Mechanisms of Governance	Incentives and valuation of data	Checks and Balances
		natural person. This act is likely to affect public sector undertaking, private sector data intermediaries and consumers.		conditions in case of personal data; re-use must be compliant with IPR, however with exception to certain provision to the database directive. For this, the commission proposes for member stated to designate a competent body and setting up of single information points to support public sector bodies which grants access to data. The commission also introduces notification requirement for intermediaries who will be involved in data exchange services. The act also introduces the concept of data altruism which could be exercised through organisations which are to be registered with competent authorities.		

Parameters for Synthesis	Rationale and Goals	Scope of Data Covered and Stakeholders Affected	Purposes of sharing and expectation of value creation	Mechanisms of Governance	Incentives and valuation of data	Checks and Balances
Singapore						
Trusted Data Sharing Framework[130]	The Framework is aimed to address concerns over trust and security hindering the mass sharing of data, despite the benefits that can be gained from leveraging large volumes and variety of data for analytics, including machine learning artificial intelligence. **This Framework is just a guide for industry and not for compliance**	For the purpose of this Framework, "data" refers to both personal and business data (derived in the process of business, including non-personal data). It states that in case of personal data, additional safeguards should be followed by the parties. This framework is intended for use in the commercial and non-governmental sectors but excludes data sharing in or with the public sector.	**The framework highlights that data sharing would help in developing Artificial Intelligence in Singapore. In this regard, the framework highlights some use cases of data sharing.**	The framework recommends that institution or organisation empowered to operate a supervisory function related to the ecosystem may be set up. Such supervisory authority - • May refer to the regulator (or other governing bodies), or industry bodies with oversight mandates or other practical influence (e.g. industry associations, standards institutes) • Usually not directly involved in data sharing, but can influence the data sharing activities through legislative reviews, issuance of the	The framework recommends for where there is a need to assess the value of data on its own (e.g. when approached by business partners for data), organisations may consider the following three key actions: **Take Stock of Own Data** - what is the kinds of data that exists like identifiable data sets, observed data, authored data, derived data. The aim should be to form a data taxonomy. **Assess Potential for Sharing** -When assessing potential use cases and data partners for the data,	This Framework introduces 6 trust Principles: **Transparency, Accessibility, Standardisation, Fairness and Ethics, Accountability and Security and Data Integrity** as foundations to forming a trusted data-sharing partnership The framework also introduces risk assessment parameters- lack of control over the use of data, lack of control of change in exchange or platform modification, insolvency and reputational risks.

[130] https://www.imda.gov.sg/-/media/Imda/Files/Programme/AI-Data-Innovation/Trusted-Data-Sharing-Framework.pdf

Parameters for Synthesis	Rationale and Goals	Scope of Data Covered and Stakeholders Affected	Purposes of sharing and expectation of value creation	Mechanisms of Governance	Incentives and valuation of data	Checks and Balances
				guidelines, standards or accreditation schemes. **The framework also proposes the kinds of data sharing models that maybe developed**. **Bilateral** – two parties agree to share data, where sharing can be one-way or two. Trust principals can be decided between the parties. **Multilateral** – three or more parties agree to share data with one another, each acting as a Data Provider, a Data Consumer or both. Trust can be established directly by the parties or institutionally. **Decentralised** – includes peer-to-peer ("**P2P**") and other	an organisation should consider all potential stakeholders in the whole value chain or ecosystem that the organisation operates in **Consider Data Valuation Approaches-** market approach, cost approach, income approach	

Parameters for Synthesis	Rationale and Goals	Scope of Data Covered and Stakeholders Affected	Purposes of sharing and expectation of value creation	Mechanisms of Governance	Incentives and valuation of data	Checks and Balances
				distributed systems. These are designed to grant control over data access and sharing to a community of participants. Participants in this community may share data on a bilateral or multilateral basis, using advanced platforms governed by a system of incentives and crowd consensus		
Australia						
Data Sharing and Release Legislative Reforms, 2019[131]	**The report forms the basis of the new regulation to be introduced for purposes of sharing of such data. It introduces the standards for a legislation that will** empower government agencies to safely share	The new legislation will empower government agencies to safely share public sector data with trusted users. **Public sector data is data held by the Australian government as it fulfils its various functions**.	Under the proposed Data Sharing and Release Legislative Reform, data sharing may occur for public benefit. The framework prescribes a purpose test to this end. This test is satisfied if sharing is reasonably necessary - to inform	The report recommends for setting up of **National Data Commissioner as an independent authority with oversight of the new data sharing system**. The Commissioner will play an important dual	Any cost and resource related matters will be part of the data-sharing agreements**.** **If the costs are to be incurred by the users, they will be informed about the same.**[132]	**The framework has proposed data sharing principles which are based on –** Data sharing is for an appropriate project or program of work

[131] https://www.datacommissioner.gov.au/sites/default/files/2019-09/Data%20Sharing%20and%20Release%20Legislative%20Reforms%20Discussion%20Paper%20-%20Accessibility.pdf
[132] https://www.pmc.gov.au/sites/default/files/publications/data-sharing-principles-best-practice-guide-15-mar-2019.pdf

Parameters for Synthesis	Rationale and Goals	Scope of Data Covered and Stakeholders Affected	Purposes of sharing and expectation of value creation	Mechanisms of Governance	Incentives and valuation of data	Checks and Balances
	public sector data with trusted users for specifed purposes. Its aim is to streamline and modernise data sharing, overcoming complex legislatve barriers and outdated secrecy provisions.	This may include data like on topics as diverse as weather patterns, who is coming and going from Australia, and administrative data about access to government services by both businesses and individuals. Such data may exist at different levels of detail, including aggregated to the category or population or at the more detailed unit record.	government policy, program and service delivery or for research and development Commercial uses of public sector data by the private sector could be limited to non-sensitive data that is openly released. The first two (government policy and programs and research and development) may involve the sharing of personal information but should result in outcomes for entire community. In contrast, the final purpose (government service delivery) will involve the sharing of personal information and support better outcomes targeted at individuals no matter what community they belong to.	role: championing greater data sharing while promoting safe data sharing practices. That framework recommends that the Commissioner should be empowered to apply strong penalties to intentional or negligent misuse and should cooperate with other regulators, including the Australian Information and Privacy Commissioner. A National Data Advisory Council will be formed, advising the National Data Commissioner on ethical database, community engagement, technical best practice, as well as industry and international developments.		Data is only available to authorised users The environment in which the data is shared minimises the risk of unauthorised use or disclosure. Appropriate protections are applied to the data Outputs are appropriate for further sharing or release Along with safeguards of Privacy Act of 1988. The report proposes of privacy by design approach in data sharing agreements and will follow the principles laid out in the Privacy Act. However, it does not give concrete view on consent and leave of National Data Commissioner. To increase transparency, the registers of Accredited Data Service Providers and

Parameters for Synthesis	Rationale and Goals	Scope of Data Covered and Stakeholders Affected	Purposes of sharing and expectation of value creation	Mechanisms of Governance	Incentives and valuation of data	Checks and Balances
				Data sharing agreements will be a requirement for all data sharing under the Data Sharing and Release legislation		Accredited Users will show who has been accredited to offer data services, to access and work with data. Include a complaints mechanism for Data Custodians, Accredited Users and Accredited Data Services Providers to raise system-specific complaints with the National Data Commissioner.
Data Exchange Framework IT Strategy Action Plan 2017-18[133]	This data exchange framework creates a standardised whole of Victorian government (WOVG) data exchange approach regardless of datatype, classification, exchange method, platform, or intended use The framework came about as support	This framework covers structured data i.e. data in the form of database with appropriate contextual information. It creates an exchange framework primarily for the government departments, however the target audience for such data can be data custodians, data owners	There are specific purposes which are stipulated, however such purpose should broadly be interest in the interest of the government, department or public in Victoria.	In this framework data requestor, will have to submit a data request which underlines the kind of data requested, purpose of use, whether such data is openly available. The request will be made to the provider after the approval from the relevant government department.	No incentive structures are defines , in case of any legal obligations with respect to data ownership contractual agreements will support creative license requirements and terms	**This data exchange framework is built-on – transparent and collaborative accountability,** data privacy, confidentiality, security and intellectual property is respected and protected during and after the exchange of date **,** data is exchanged with assurance provided for the

[133] https://www.vic.gov.au/sites/default/files/2019-07/Data-Exchange-Framework_0.pdf, https://www.vic.gov.au/sites/default/files/2019-09/Data%20Exchange%20Guideline.PDF

Parameters for Synthesis	Rationale and Goals	Scope of Data Covered and Stakeholders Affected	Purposes of sharing and expectation of value creation	Mechanisms of Governance	Incentives and valuation of data	Checks and Balances
	Victorian Centre for Data Insight's (VCDI). Data Reform Strategy, API (application programming interface) gateway.	etc. Hence, the framework focuses more on government to government and non - government sharing.		Such requests will then be assessed under the Privacy Act 1988 (Cth),Victorian Data Sharing Act 2017, Public Records Act 1973 and Freedom of Information Act 1982. If there is no legal mandate to share the data contract agreement will be formulated. Every data request will be assessed based on risk based assessment and most data should be made unindentifiable.		appropriate use of data after the exchange
Japan						
Contract Guidance on Utilization of AI and Data by Ministry of Economy Trade and Industry 2018[134]	IoT and AI, data use is expected to create new value added and solve societal issues through data collaboration that transcends business boundaries. It is often	The guidelines divide the contracts into different categories based on the purpose of sharing and include different kinds of data based on that –	Different contracts based on the purpose of data sharing – From one data provider to another – The purpose for which data is not allowed	Data sharing would be governed by contractual terms for models of sharing which would include data sharing from one data provider to another, creation and	**Contractual terms would specify licensing terms and profit sharing** in case the data is created by multiple parties.	The guidance recommends for clauses to be included in the contract with regards to –

[134] https://www.meti.go.jp/english/press/2018/0615_002.html, https://www.meti.go.jp/press/2019/04/20190404001/20190404001-1.pdf.

Parameters for Synthesis	Rationale and Goals	Scope of Data Covered and Stakeholders Affected	Purposes of sharing and expectation of value creation	Mechanisms of Governance	Incentives and valuation of data	Checks and Balances
	difficult, however, for businesses to conclude contracts related to utilization of data or AI technology **due to lack of sufficient experience in contract practices and the gaps in understanding between the parties involved.** **The guidelines highlight on the questions and details that should be formulated while contracting for data sharing.**	**From one data provider to another** - whether to use derivate data or not, **notice to be given when data includes personal information.** **Where data is newly created due to the involvement of multiple parties** – only the parties involved in data creation can use, their might be restriction on sublicensing to third parties. **Sharing data through the platform** – type of data to be specified	to be used should be mentioned. Where data is newly created due to the involvement of multiple parties – terms of usage between the parties is to be specified Sharing data through the platform - describing usage range of data or scope of usage in the agreement.	sharing of data by multiple parties or creating a data sharing platform. Contracts for any these models would include clauses such as – **Responsibility for disputes with third parties due to provided data** **Scope of license to use provided data.· Guarantee / non-guarantee of data**. **Liabilities of platform operators.· Liabilities of data providers and users.· at withdrawal / termination**	Additionally analysis for exploring the intellectual property and ownership rights on data have already been undergoing since 2019, with a study group step for exploring intellectual property rights in the fourth industrial revolution.[135] **There is no specific costing mechanism** prescribed for the data	**Notices when data includes personal information,** Management method, security Liabilities of platform operators. Liabilities of data providers and user
Act on Special Measures for	This act had been enacted at the backdrop of Japan's economic	This act includes both public and private sector information (excluding	On energy, industrial machine and logistics and to solve social problems	The Act establishes a certification system for business plans that aim	**There is no specific incentive structure specified in the Act.**	In case the data contains the personal information as under the Act on the

[135] https://www.meti.go.jp/english/press/2017/0419_001.html

Parameters for Synthesis	Rationale and Goals	Scope of Data Covered and Stakeholders Affected	Purposes of sharing and expectation of value creation	Mechanisms of Governance	Incentives and valuation of data	Checks and Balances
Productivity Improvement, 2018[136]	policy of 2017, which aimed at attracting investment, and facing international competition and to increase productivity in the IoT, big data and artificial intelligence. Notably, the provision under this act are subject to the Basic Act on the Advancement of Public and Private Sector Data Utilization[137] and Act on the Protection of Personal Information	information that is likely to damage national security, hinder the maintenance of public order, or be an obstacle to the protection of public safety)	like accident prevention, energy management	at data sharing or collaboration, allowing certified business operators to take advantage of tax breaks and other measures for investing in facilities, equipment and so on used for efforts stipulated under the Act. In addition, the Act is to establish new procedures through which data sharing business operators who receive confirmation in terms of predetermined levels of cyber security, are eligible to request that the government, independent administrative agencies and other public entities provide them with necessary data.	**However, the Act proposes to give tax breaks to business operators who are certified and make a plan for innovative data use.**	Protection of Personal Information, the minister and authority concerned will examine the application appropriately and liason with Personal Information Protection Commission . It will also examine the necessity of prompting such use of information
Netherlands						

[136] https://www.meti.go.jp/english/press/2018_06/0606_001_00.html
[137] http://www.japaneselawtranslation.go.jp/law/detail/?id=2975&vm=02&re=

Parameters for Synthesis	Rationale and Goals	Scope of Data Covered and Stakeholders Affected	Purposes of sharing and expectation of value creation	Mechanisms of Governance	Incentives and valuation of data	Checks and Balances
Dutch Digitalisation Strategy : Dutch Vision on Data Sharing Between Businesses 2019[138]	**The strategy recognises that data is a resource for the 21st century and its re-use and sharing will benefit business. However, it recognises that the government can play a role in this if the markets itself have failed to do so and to reduce the risk of privacy breaches and ensuring cyber - security in data sharing. Additionally, the strategy is inspired by the analysis of the used cases of data sharing in the Netherlands following different arrangements and principles.**	The strategy **covers personal, non-personal and data generated out of equipments** and recognizes that such data can be shared amongst business with proper compliance and agreements.	The strategy covers data **sharing for innovation and increasing competition**. It also recognizes that **compulsory data sharing maybe introduced for sharing of data for public interest** such as competition, freedom of choice, innovation, good health or free-flowing traffic and green economy.	**The strategy first and foremost encourages voluntary data sharing based on the principles of FAIR (data must be findable, accessible, interoperable and reusable)** through sets of agreements between parties and common technical principles. The government may facilitate such sharing through proper infrastructure. The strategy recognises the need for **mandatory data sharing only for public interest purposes** when data cannot be easily produced or gathered; it is not possible to make appropriate sharing agreements; and such an obligation would not	This will be determined through contractual agreements between the businesses agreeing to share the data. The strategy recommends that such sharing agreement must **specify the intellectual property clauses, trade secrets, ownership of data within such agreement.** In such cases the government will only play a facilitators role. Even for the cases where mandatory sharing maybe proposed the strategy suggest that due attention needs to be	**The strategy specifies that while sharing data the rights and obligations must be clearly specified-** - **Sharing of personal data should be in compliance with the GDPR** - **Frameworks related to consumer law where relevant must also apply**

[138] https://www.government.nl/documents/reports/2019/02/01/dutch-vision-on-data-sharing-between-businesses

Parameters for Synthesis	Rationale and Goals	Scope of Data Covered and Stakeholders Affected	Purposes of sharing and expectation of value creation	Mechanisms of Governance	Incentives and valuation of data	Checks and Balances
				reduce incentive for innovation, consequences for intellectual property and necessity to obtain the consent of the data subject.[139]	given to its effect on intellectual property	
United Kingdom						
National Data Strategy 2020[140] (Under Consultation)	This strategy looks at how to leverage existing UK strengths to boost better use of data across businesses, government, civil society and individuals. The strategy focuses on using data to deliver new and innovative services, promote stronger competition, and better prices and choice for consumers and small businesses.	The strategy refers to data as information about people, things and systems, which means it includes both personal and non-personal data.	They have identified five concrete and significant opportunities for data to positively transform the UK in following domains: 1. Boosting productivity and trade 2. Supporting new businesses and jobs 3. Increasing the speed, efficiency and scope of scientific research 4. Driving better delivery of policy and public services	The strategy does not recognise any concrete mechanism for governance and proposes for exploration of government as a collaborator, steward, customer, provider, funder, regulator and legislator. The strategy of open for consultation and it proposed to get views of the stakeholder on kind of government intervention that might be apt.	**While no definite valuation mechanisms is proposed, the strategy observes that** aim should be to maintain and bolster a data regime that is not too burdensome for the average company – one that helps innovators and entrepreneurs to use data legitimately to build and expand their businesses, without undue regulatory	**The strategy to build on Data Ethics Framework published by the government and ensure to maintain transparency in the AI use of data.** It also aims to ensure that any governance model would ensure privacy of consumers and intellectual property of businesses.

[139] The strategy prescribes for a decision tree under which the government will first as ask : Does data sharing offer opportunities in regard to (for example) productivity and innovation, competition and choice, or societal challenges?-Will data sharing take place in markets and communities even if the government does not take a role?- Could private data sharing come about with targeted financial and/or organisational assistance? And then decide on its role.

[140] https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy#data-1-3

Parameters for Synthesis	Rationale and Goals	Scope of Data Covered and Stakeholders Affected	Purposes of sharing and expectation of value creation	Mechanisms of Governance	Incentives and valuation of data	Checks and Balances
	This strategy comes at the backdrop of **used cases of data sharing by private companies and amongst various sectors, which has also inspired the parameters and focus of this strategy.** Moreover, the strategy also notes that government has considerably invested in research and partnered with organisations with expertise in the field to develop and test models of data sharing.		5. Creating a fairer society for all.	It specifically notes that mechanisms to make the data available should ensure that appropriate balance is struck between maintaining incentives to collect and curate data, and ensuring that data access is broad enough to maximise its value across the economy.	uncertainty or risk in the UK and globally	
UK AI Sector Deal (Data Sharing Infrastructure)[141][142]	This Sector Deal sets out actions to promote the adoption and use of AI in the UK, and delivers on the recommendations of the independent AI review, 'Growing the AI industry in the UK'. The	It includes both personal and non-personal data. Although, in the case of personal data consent need to be taken along with appropriately informing the use of how his/her data will be used. Alternatively such	No specific purpose of setting up data trusts have been identified. However three pilot have been initiated with – • the Greater London Authority and the Royal Borough of	The AI Sector Deal proposed for a data trust model for un-tapping the data sets from both public and private sectors. Data trust are defined as: 'a legal structure that provides independent	In the pilots conducted, broadly the incentive to contribute to the data trust rested in – delegate data steward responsibilities i.e. costs related to sharing of data goes to the data trusts,	The proposed data trusts have to comply with rules and regulations with respect to privacy , however in the case of no legal rule ' consent of the governed' would be the

[141] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/702810/180425_BEIS_AI_Sector_Deal__4_.pdf
[142] https://docs.google.com/document/d/118RqyUAWP3WIyyCO4iLUT3oOobnYJGibEhspr2v87jg/edit#

Parameters for Synthesis	Rationale and Goals	Scope of Data Covered and Stakeholders Affected	Purposes of sharing and expectation of value creation	Mechanisms of Governance	Incentives and valuation of data	Checks and Balances
	strategy proposed for setting up of data trust to tap on datasets help by public and private sector. It was also pointed by the report published by the UK Digital Competition Expert Panel - Unlocking digital competition report', which identified that increasing access to data – potentially through data trusts – can be a regulatory tool to improve competition	data could anonymised or aggregated.	Greenwich to explore the creation of a data trust in an **urban space**, focusing on data about electric vehicle parking spaces and data collected by heating sensors in residential housing. • WILDLABS Tech Hub to explore the creation of a data trust to tacklethe **international illegal wildlife trade**, focusing on image and acoustic data, and data acquired by officials at borders. • food and drink manufacturers and retailers to explore the creation of a data trust to tackle **global food waste**, focusing on food waste and sales da	stewardship of data. Under this data trust are independent collaborations or organisations, which become stewards of data. A data trust can decide who can access the data and for what purpose. This was piloted in three sector in Europe to consider the viability of the system	data trusts then also become responsible for mediating between prospective data users, data trusts would also engage with citizens and consumers, sharing data might create more efficiency in products, services and supply chains, reputational benefits for companies for giving some data and enhance consumer trust, financial returns as data trust can be designed in a way to create remuneration and responsibility on trust for compliance of regulation. In its design the data trust in-fact proposes for model through which data holders can make arrangements with data trusts on incentive strutures. Additionally intellectual property rights in the data will be licensed or transferred	norm to be followed by the data trust authority.

Parameters for Synthesis	Rationale and Goals	Scope of Data Covered and Stakeholders Affected	Purposes of sharing and expectation of value creation	Mechanisms of Governance	Incentives and valuation of data	Checks and Balances
					based on agreement between data holder and data trusts.	
Sectoral Data Sharing Frameworks						
Finland						
Act on the Secondary Use of Health and Social Data, Finland 2019[143] (the Act)	he objective of the this act is to facilitate effective and safe processing and access to the personal social and health data for steering, supervision, research, statistics and development in the health and social sector. A second objective is to guarantee an individual's legitimate expectations as well as their rights and freedoms when processing personal data.	The Act stipulates for the following kinds of data to be shared - • data from several different controllers is combined • the register data originates from private social welfare and health care service providers • the data is stored in Kanta services (data base of medical records and other related information).[144]	The **data permit requests are clearly required to stipulate the purposes of data sharing, data utilisation plan** and after the assessment of such purposes with the authority grants data permits. Along with this they also have to specify what controller of data they want to target.	**The Act stipulates for the creation of Health and Social Data Permit Authority (FinData).** The Authority gives access to data after permit requests are made and processed by it. If the permit is processed they gather data from a controller or request from a private service provider and then combine, pseudonymise and anonymise the data or produce statistical data converting and	Pricing of the processing permit request include the costs of - 1. Fee for Findata for data request or data permit 2. Costs incurred by data controllers for the extraction and delivery of data, based on each controller's own regulations 3. Working hours used by Findata for combining, pre-processing, pseudonymising	The Act requires compliance with GDPR

[143] https://stm.fi/documents/1271139/1365571/The+Act+on+the+Secondary+Use+of+Health+and+Social+Data/a2bca08c-d067-3e54-45d1-18096de0ed76/The+Act+on+the+Secondary+Use+of+Health+and+Social+Data.pdf
[144] https://www.kanta.fi/en/what-are-kanta-services

Parameters for Synthesis	Rationale and Goals	Scope of Data Covered and Stakeholders Affected	Purposes of sharing and expectation of value creation	Mechanisms of Governance	Incentives and valuation of data	Checks and Balances
		All the data is to be anonymised or pseudoynomised		combining the permit holder's own data.	and anonymisation the data 4. Remote access environment charge for data permit holders.	
Sectoral Level Framework/ Initiatives/Strategies for Data Sharing						
International/ Global Initiatives						
Dawex[145]	Dawex Data Exchange and global marketplace allows users to deploy free or monetized business models and multiple use cases including internal data exchange, data sourcing, free data sharing, open data, data monetization and data marketplace orchestration between customers, suppliers, partners, subsidiaries	This global data marketplace **hosts all kinds of data aggregated data, missed datasets etc**. However, all the data is encrypted and is hosted at servers closest to location of the organisation -North America, South America, Europe or Asia with technical infrastructure meeting the strictest worldwide standards.	The users of the market places are free to set purpose of usage conditions on the data. The marketplace also provides pre-set contracts for this. While the marketplace caters to all industries there are specific focus industries stipulated – Agriculture Automative	**Its an open market place, where data can be monetised, shared according to specific business models of organisations/companies**.	The marketplace can be joined for free, however the valuation of the data will have be determined by the users themselves. There are different kinds of packages available on the platforms for increasing the valuation and making data visible to more people. –	To secure your data exchanges beyond national borders, Dawex has chosen to obtain certification from independent data protection authorities. They follow Privacy by Design concept in their marketplace They ensure compliance with GDPR and help their customers comply as well.

[145] https://www.dawex.com/en/

Parameters for Synthesis	Rationale and Goals	Scope of Data Covered and Stakeholders Affected	Purposes of sharing and expectation of value creation	Mechanisms of Governance	Incentives and valuation of data	Checks and Balances
	and many other organizations. They note the necessity of such marketplace on account of – Many organisation and companies are already launching specialised marketplaces in different regions Governments are supporting such initiatives Governments are also adopting regulations such GDPR and other data flow regulations Associations are already building new forms trust data sharing models.		Bank Insurance and Financial Services Energy Retail and Consumer Goods Health Environment Media and Entertainment Public Sector Shipping and Logistics Tourism and Sports		Community- Free joining of the market place Business – fee per month Enterprise - customised pricing Regarding data usage rights between parties licensing contracts could be set-up	
International Data Spaces Association[146]	International Data Spaces is run by International Data Spaces Association via an European non-profit,	It includes **all kinds of data including both personal and non-personal data, however IDS adheres to**	IDSA is suitable for almost every industry. The orientation of its members is wide-ranging, from medium-	The data provider – i.e. the company – determines who may use the data and how to use them. As a result,	Each business is free to propose its own valuation and pricing models.	**Data security and data sovereignty are the essential features of Industrial Data Spaces**.

[146] https://www.internationaldataspaces.org/our-approach/#about-us

Parameters for Synthesis	Rationale and Goals	Scope of Data Covered and Stakeholders Affected	Purposes of sharing and expectation of value creation	Mechanisms of Governance	Incentives and valuation of data	Checks and Balances
	which takes an active part in designing a trustworthy architecture for the data economy. More than 101 companies and institutions of various industries and sizes from 20, global acting medium-sized companies, software and system houses are members of the association. The IDSA aims to guarantee data sovereignty by an open, vendor-independent architecture for a peer-to-peer network which provides usage control of data from all domains	**European principles of privacy and data security**.	sized businesses to multi-corporate enterprises: from urban data space to material data space, medical data space, mobility data space, etc For the exchange of data IDSA architecture creates different roles for different parties which include - Data Provider, Data User, Data Broker,	partners in a value chain can individually or jointly access certain data by mutual agreement in order to start something new, develop new business models, design their own processes more efficiently or otherwise initiate additional value creation processes. **Each participant and each component in this network is certified and can be identified as a conclusive identity. Certification prescribes and verifies the implementation of generally accepted safety standards and mechanisms. The participants in the data space are obliged to observe both the general rules for dealing with each other**		Data owners can always keep control over their data and can also fulfil their own standards of data security. The data are exchanged safely on demand, if they are requested by certified, trustworthy partners. The main feature of the International Data Spaces is that data providers – i.e. companies that want to make their data available for digital services – can always keep control over their data and enforce their own standards of data security (keyword: "Privacy Enforcement"). The data remain with their provider and are exchanged securely on demand. They are only exchanged if they are requested by certified, trustworthy partners. If

Parameters for Synthesis	Rationale and Goals	Scope of Data Covered and Stakeholders Affected	Purposes of sharing and expectation of value creation	Mechanisms of Governance	Incentives and valuation of data	Checks and Balances
				and the data usage guidelines specified by the data providers. IDS provides technologies to implement and control this at a technical level (usage enforcement)		necessary, the data themselves are not exchanged, but analysis procedures are applied to the data.
Netherland						
iShare[147]	The iSHARE project is an initiative of the Neutral Logistics Information Platform (NLIP), which is the leading platform promoting data exchange in the transport and logistics sector and part of the Netherlands' Logistics Top Sector programme. The iSHARE uniform set of agreements for identification,	iSHARE is developed in conjunction with organisations that represent a cross-section of the sector: all modalities, organisations of all shapes and sizes, public-sector and private-sector organisations, data providers/data recipients and their software suppliers. Before becoming the part of the ishare platform, the organisation requires the companies to sign	The participants in the scheme – which include more than 20 public and private organisations – focus on how to share information as effectively as possible. **By building agreements and standards together, they have created an atmosphere of trust.** The conditions for data use are recorded in the agreements system. The data owner's authorization specifies the purpose for and the conditions under	Once an organisation has an iSHARE identity they can use it to authorise the data hub to release data to third parties. In the iSHARE authorization you specify which party is permitted to access which data. If the situation changes, you can withdraw or modify your authorization. Through the data hub all parties and organisation then have digital access to the data of the owner and also to that of many other contracting parties.	These condition maybe stipulated in the contracts, however, no explicit incentive or valuation of data has been prescribed	**The ishare agreements ensure compliance with the GDPR and other applicable legal obligations.** It also gives complete control of the data to the owner and they can withdraw from sharing at any time.

[147] https://www.ishareworks.org/en/ishare

Parameters for Synthesis	Rationale and Goals	Scope of Data Covered and Stakeholders Affected	Purposes of sharing and expectation of value creation	Mechanisms of Governance	Incentives and valuation of data	Checks and Balances
	authentication and authorization enables everyone to share data with everyone else in the logistics sector in a simple and controlled way – including with new and hitherto unknown partners. Through iSHARE, NLIP is keen to eliminate data-sharing barriers, to stimulate supply chain collaboration and to scale up, accelerate and successfully connect existing digital data-exchange initiatives. This initiative have been supported by relevant Dutch Ministeries.	standardised **agreements for data sharing in which type of data to be shared, with whom it is to be shared and licensing terms are specified.** **Once the organisation/company is issued an ishare identity they can share and access data through data hubs organised by ishare**	which his or her data can be used. Some of the beneficiary categories which have been identified include – Freight Forwarders Platforms Shippers Software Suppliers Transport Companies	A precondition is that they also have an iSHARE identity. A machine-to-machine link, for example in the form of an API, is also required to receive the right data rapidly, securely and entirely automatically.		

ANNEXURE III

CUTS Comments on the Previous Version of the Report

1. Standards of Anonymisation

1.1. 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 re-identification is changed. Most importantly, over-anonymization can render datasets useless for further analysis or innovation. 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.

2. Non- Personal Data Authority

2.1. 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.

2.2. 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.

2.3. 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.

2.4. 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.