Future of Non-Personal Data Governance in India

A Consumer Perspective

Introduction

It has been said that the 21st century will be of those who will have the most data. So much so that consultants, policymakers, institutions and governments have been jolted into action to realise economic value out of data.

India is one such country that has been trying to figure out how to derive public and economic value from data. While India is still deliberating upon its Personal Data Protection Bill, it has already taken steps to ascertain the governance mechanisms for non-personal data (NPD) by forming a Committee of Experts (CoE) to propose a regulatory framework for NPD.[1] Over the last few months, the committee has released two public reports, the revised report being significantly more progressive than the first one. However, several concerns persist, which might have significant consequences on the future of data governance in India if the proposed framework is adopted in its current form.

The NPD Governance framework aims to unlock the value of data in a way that leads to the fulfilment of 'public interest purposes' through establishing a community rights framework. At the same time, it needs to be acknowledged that consumers are the originator of data and their interests are intertwined at every step of the data value chain. Thus, it is important to keep consumers at the centre of data governance deliberations.

Apart from the NPD governance framework, there also have been sectoral level initiatives such as the Data Empowerment and Protection Architecture (DEPA) and National Health Data Management Policy, which have also prescribed conditions of consent and data management mechanisms that would inadvertently affect consumers. Along with this, there already has been open data initiatives and strategy for national open digital ecosystems (NODE), which aims is to increase data access to citizens. Overall, as the policy ecosystem for data evolves consumers would play a critical role in its sustenance and efficacy.

In light of the evolving mechanism of data governance and its effect on consumers, this policy brief highlights key issues emanating in the data governance ecosystem from the lens of the NPD Governance Framework proposed by CoE. These issues are discussed at length from a consumer perspective, taking into account the evolving data protection and sharing frameworks in other jurisdictions, to build context and a way forward.

Key Assessments

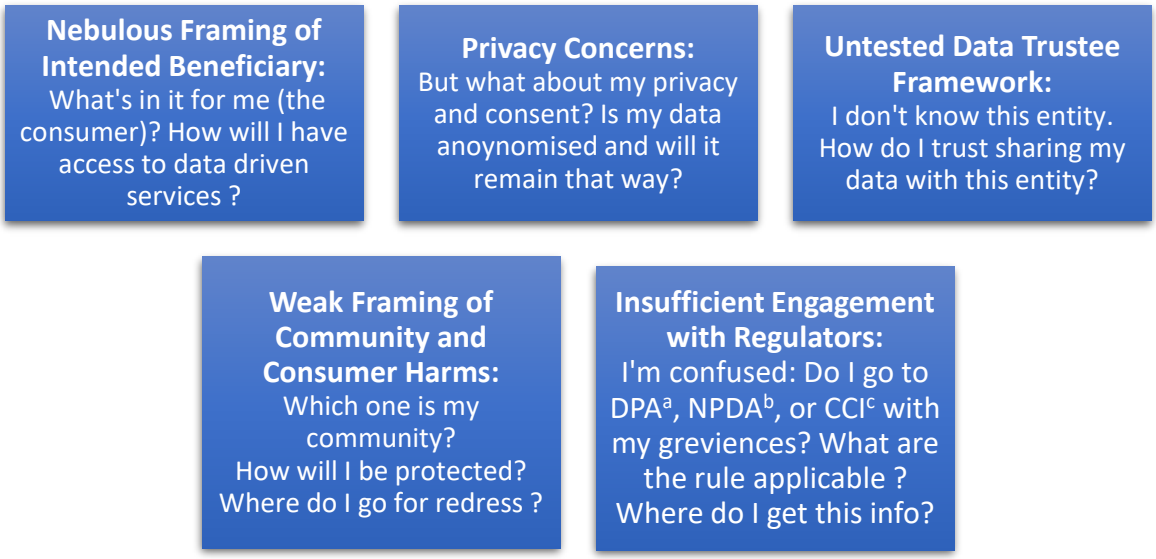

FIGURE 1: KEY ASSESSMENTS FROM A CONSUMER PERSPECTIVE

[a] Personal Data Protection Authority [b] Non-Personal Data Authority [c] Competition Commission of India

1. Nebulous Framing of Intended Beneficiary

The revised report on NPD Governance Framework (the Report) focuses on achieving 'public interest purpose' and enforcing the rights of the community in NPD. The CoE envisages that through such a framework, the benefits would flow not just to the organisations that collect the data but also to the community to whom the data belongs. Such rationale is noble and is a step in the right direction, however, time and again it is being observed that the term "public interest" in itself is broad and it is very difficult to ascertain who is the "intended beneficiary" of such objective.[2]

This is because certain questions remain unanswered such as - how will this public interest incorporate the interest of marginalised communities; in cases where data is used for new business operations, how will it be ensured that the business is in the interest of the community; how it can be ensured that data-driven services reach the consumers; how to define community.

This vagueness becomes heightened as the data principal is the originator of the data and is also the ultimate consumer of the data and as such the 'community' only comes into existence post-facto, depending on the representation that the dataset portrays. This provides a vague antecedent of assurance that consumers would become part of a community that will be the ultimate beneficiary, negating a possibility of exclusion errors and circumstances in which individuals may have conflicts with larger community interests. Moreover, organic

identification of the community is difficult to determine, which can make balancing community interest with individual interests difficult.

Even the Report prescribes a very ambiguous definition of community, which can create conflicts and overlaps. This is specifically true in the Indian context, wherein one person may form part of multiple communities based on their gender, caste, religion, or income group, thus it becomes problematic to accurately define benefit transfer. For example, a Dalit woman may be identified to be part of a particular gender and also a caste category, which makes it difficult which identity should be given prominence in the transfer of benefits.

Furthermore, exclusion and inclusion errors occur in public property regimes when those who already have resources are better able to extract benefits out of public goods rather than those who are actually in need.[3] This phenomenon is closely related to power dynamics and those who have more control over decisions are the ones who are favoured by public interest policies. We have already observed this phenomenon in the case of Aadhaar, wherein exclusions were created due to errors in fingerprints, poor internet connectivity, and seeding errors, etc.[4] These reflections are useful in determining the application of 'public interest purpose' and the related possibility of exclusion errors.

Moreover, this reflects gaps in institutional, infrastructure capacity in formulating new frameworks, negating the needs of the demography. In these cases, the capacity of consumers or even the community to extract the intended benefits also plays a crucial role. These problematic dichotomies indicate that the path toward providing benefits from data access to citizens is unclear as it presents the risk of data concentration leading to inequitable distribution of data.[5]

2. Privacy Concerns

The Report has tried to identify and address privacy concerns for the consumers or the data principals, however, certain concerns remain. The Report goes on to assume that the moment when personal data becomes NPD, the frameworks tend to treat it with less sensitivity and less prone to risk, which is a false assumption. NPD is just as prone to risk as personal data, if not more.[6] For example, profiling risks could be created, when datasets are treated at an aggregate level.[7]

Some of these issues are not just limited to this report but also extend to other frameworks such as Data Protection and Empowerment Architecture (DEPA), National Health Data Management Policy, and the Personal Data Protection Bill 2019 (PDP Bill). These concerns pertain to –

2.1. Binaries between personal and NPD

The Report defines NPD as data devoid of Personally Identifiable Information (PII) and is not personal data, however, creating any such binaries without clear concepts of privacy

established by data protection principles becomes problematic. In this regard, the European experience suggests a context-specific definition of personal data.[8] Similar observations were also made, in the privacy perception survey conducted by CUTS, which highlighted the need to include user perception and perceived sense of users' intimacy and necessity related to data in the test of 'identifiability'.[9]

More recently, researchers have warned that with technological evolution, such as improvement in re-identification techniques and legal precedents, a lot more data that was previously considered as NPD will come within the category of 'personal data'.[10] Thus, creating binaries and identifying where in the process NPD can become personal data becomes problematic creating privacy risks.

Moreover, in this context, studies[11] and a detailed analysis conducted by the Article 29 Working Party[12] while establishing standards for GDPR have indicated that the level of anonymization differs with different techniques and tools, thus the susceptibility of re-identification also changes**.** Along with this, recent research has also pointed that any anonymization technique cannot be full-proof.[13] Thus, over-reliance on anonymization techniques to create these binaries may also be flawed.

2.2. Consent Mechanism

The issues related to consent architecture are not limited to the NPD framework and extends to other frameworks. The CoE 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 and observed that users do not read privacy policies (notices) due to their length, legalese, complicated and unfamiliar language.[14]

Despite the clear evidence of consent mechanism not truly empowering consumers, the Report further adds 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. This also creates an information asymmetry as the purpose of anonymisation cannot be specifically determined ex-ante, which dilutes the objective of making informed and clear consent as has been prescribed in the PDP Bill.

3. Untested Data Trustee Framework

The Report proposes for 'data trustees' as intermediaries between the community, data custodians, and data requestors. In doing so, it places the responsibility on these intermediaries to control the flow of benefits and defining public interests. Along with this, DEPA and PDP Bill have also introduced intermediaries in the form of consent aggregators and consent dashboards.

However, considering very limited used cases of such intermediaries in India and with the crucial responsibility that they are to handle, without laid down principles of "duty of care", increases the risk of community and consumer interest being misrepresented. In this context, we must also be aware the "duty of care" is highly context-dependent, and with the untested nature of these intermediaries establishing the principle for duty of care also become complex.

At the same time, we should recall lessons learned from the Indian experience with a public-private partnership model, on which, the Kelkar report cautioned that such models may be used by the government to evade responsibility and accountability, therefore, citizens' interests should be at the core of such frameworks.[15] With 'data trustee' being delved with the responsibility of processing data requests without specific accountability mechanisms or independent financial sources, the risk of bias towards dominant private interest may emerge, forgoing the interest of consumers and small and medium enterprises.

And, with new untested platforms such as consent aggregators and dashboards with uncertainty about their interaction with consumers presents a possibility to fester mistrust.[16] It may also increase the risk of governance exclusions[17], in which, certain community' interests may not be adequately represented if they are not able to interact or approach the intermediary in an adequate manner.

4. Weak Framing Harms and Grievance Redress

The report recognises that there could be privacy harms as well as active and accidental harms from sharing NPD. However, no specific meaning is being assigned to these terms. Additionally, there is also less consideration to the collective harms that may emerge from combining various datasets, which would go beyond privacy risks and may include differential pricing, manipulative target advertising, exclusion and inclusion errors.

Thus, not adequately providing specific definition or guidelines related to harms, puts a burden on consumers and the community to establish the causality of these emerging harms from combining datasets.[18] Such problems have also been identified in the context of the PDP Bill, where the onus of identifying and establishing, which category of harm is likely to be incurred is on the consumers.[19]

Moreover, while the report states that appropriate grievance redress mechanisms[20] would be set up to address concerns by the data trustees, however, without a clear prescription and understanding of harms, and approachable avenues for redress, communities or consumers would not be able to indulge with redress mechanisms. This was also highlighted in a CUTS survey, which observed that most consumers are not aware of avenues for grievance, and only half of those who have earlier experienced a privacy breach went on to complain about it.[21]

Such issues will dilute the community benefit objective and place consumers at the margins of the data sharing value chain, without any necessary recourse. Overall, this points to insufficient focus on the onus of the government, regulators, and intermediaries to create an environment where consumers feel empowered to contest the decision at various levels.

5. Insufficient Engagement with Regulators

As envisaged by the Report, the Non-Personal Data Authority (NPDA) has both enabling and enforcing functions in governing NPD access. In this context, while the Report states that the NPDA will be created in consultation with industry and other regulators, there are missing mechanisms, through which the community and the consumers can themselves engage with the regulator to build greater trust in the authority. The responsibility of grievance redress has also been shifted to the data trustees, and not the NPDA, creating multiple points of enforcement, which also extends to the Data Protection Authority, Competition Commission of India (CCI). This may lead to more confusion for the consumers, regarding which authority to approach.

6. Data Access by the Government

Another pertinent concern emanates from increasing data access exemptions, which have been given to the government such as under sovereign purposes prescribed the Report and similar kind of access are also stipulated by recently released Intermediary Guidelines[22] and Section 35 & 36 of the PDP Bill.[23]

This access is given without appropriate safeguards of necessity, proportionality and legality of data use, creating risks of overreach, surveillance and curbing the right to free speech and expression. These exemptions are also in line with the proposed exemptions for the state under the PDP Bill 2019. Moreover, the data access by the government can take the role of both normative public interests and it may also be used by law enforcement agencies, however, lack of due process and safeguards may create spill-overs and overlaps in both. Such access must be under strict scrutiny in the form of a three-pronged legal test and by ensuring purpose limitations while also narrowing down and clearly defining the exemptions.

Multi-Jurisdiction Comparison

Jurisdictions across the globe that are trying to derive the economic value of data have been relying on the policy and market maturity that they have obtained over the years. These efforts have also consciously taken a holistic perspective of all relevant stakeholders while coming up with a policy. There has been a conscious effort in several of these regulations to ensure that consumer rights and welfare are of utmost priority in trying to enable value addition of data into their economies. Through this comparison, we want to highlight some of the "good" practices, which could be adopted.

1. European Union

The European Union has had a long history of data regulations that work in tandem with each other to provide data rights to individuals while contributing to the data economy of the member countries. The European Commission has introduced the European Strategy for Data in 2020.[24]

The strategy empowers data principals by giving consumers control of their data through tools and means to take granular decisions about their data. For this, they have proposed to set up a dashboard, through which consumers can track where their data is flowing. Further, the strategy proposes to enhance the portability rights for individuals under personal data regulation and to curb difficulties in its implementation. This directive provided for the re-use of public documents for all purposes while promoting competition.

In late 2020, the European Commission also introduced the Proposal for a Regulation on European data governance (Data Governance Act).[25] The regulation provides for data usage and access, ensuring the rights of data holders, including the right to privacy, and intellectual property rights are protected. One of the primary learning for India from EU data laws and

policies pertains to its strong open data initiatives at both umbrella and sectoral, which has not led to avoiding data concentration but also increasing data access to citizens.

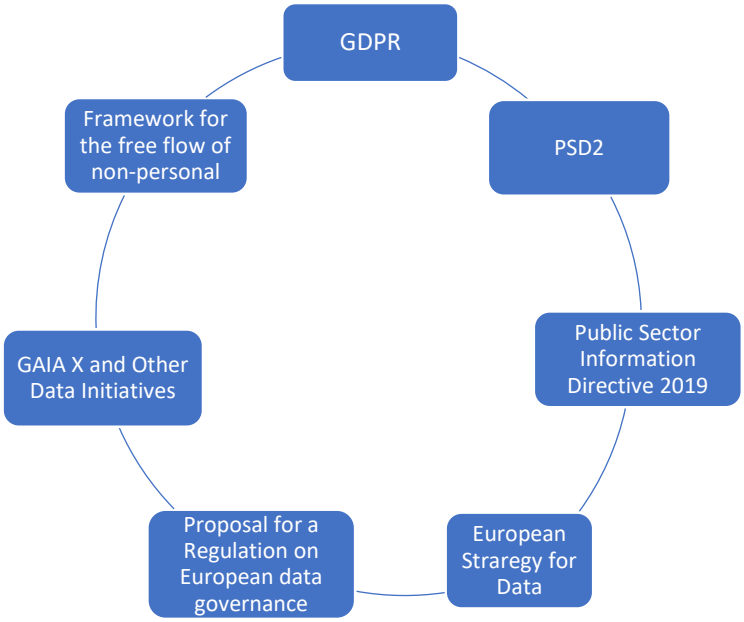

FIGURE 2: EUROPEAN DATA GOVERNANCE POLICIES

2. Singapore

The government of Singapore introduced the Trusted Data Sharing Framework in 2019.[26] It relied on the Personal Data Protection Act from 2012 to cover the aspects of personal data in the broader governance framework. The Trusted Data Sharing Framework introduced six new principles for a trusted data-sharing partnership, as indicated in Figure 3. It also illustrates, how these principles could be applied.

For example, to maintain fairness and ethics in sharing *data, it states that it would help if there is greater transparency as to the nature and sources of that data, along with greater accountability from data service providers as to the basis, on which such data has been gathered and processed*, to be stated in the contract of data-sharing.

In contrast, while the Indian NPD framework recognises the "duty of care" in handling data, it does not specifically state what this duty constitutes. The Singaporean framework goes on to introduce risk assessment parameters such as lack of control over the use of data, lack of control on platform modification, insolvency, and reputational risks. The framework indicates the way, in which a balance could be maintained between facilitating private-sector data sharing and preventing risks and ensuring secure data sharing, which are essential for fostering consumer interest. This balance seems to be missing in the Report as while it attempts to protect community interest, the main focus is establishing data as an economic resource, forging other dimensions of risk and security, which require more deliberation.

FIGURE 3: CORE PRINCIPLES OF SINGAPORE'S DATA SHARING

3. Australia

The Australian government introduced the Data Sharing and Release Legislative Reforms in 2019, which forms the basis of the new regulation to be introduced to share such data.[27]

It lists out standards to share public sector data with trusted users for specific purposes while ensuring that the innovation is fostered. The report focuses on minimising the risk of unauthorised use or disclosure of data by applying protections and creating a trusted ecosystem for sharing. For this, the framework introduces five factors to be considered while managing data-sharing - project, data, settings, people, and outputs. It aims to apply these factors to answer questions -- *how detailed the data is, will the data be used in a safe and secure environment, who will use the data, and can the project results be published without identifying individuals or businesses.*

It also stipulates for purpose limitations, in which the necessity, proportionality of using data need to be justified. These stipulations have been based on the existing privacy laws, which have not only established principles but also provided a baseline for defining the terms and processes involved.

The Report relies heavily on the Privacy Act of 1988 to propose the privacy principles and to propose privacy by design approach in data sharing to ensure utmost privacy protections for users.[28] The report had also proposed mechanisms to enhance the transparency in data sharing and its allied services. Further, there are ample checks and balances, along with grievance redressal mechanisms under the proposed authority of the National Data Commissioner. The report also left room for the states to come up with their data policies based on the established principles.

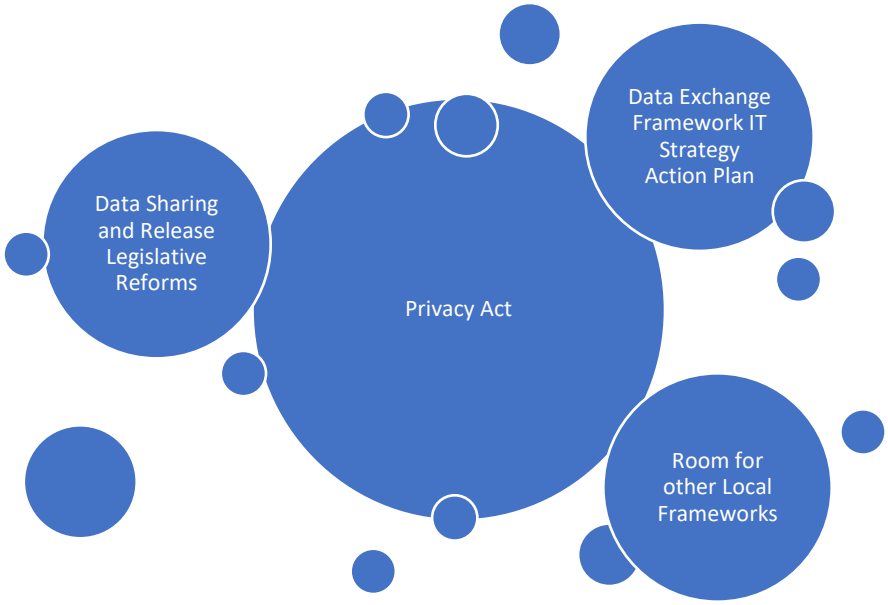

FIGURE 4: AUSTRALIAN DATA SHARING POLICIES AND ENABLING SPACES FOR LOCAL AND SECTORAL SHARING

4. United Kingdom (UK)

UK introduced its national data strategy[29], which aims to establish an all-encompassing data strategy that aims to leverage existing strengths of the UK to boost better use of data across businesses, government, civil society, and individuals. The strategy places specific reliance on the responsibility to drive trusted and safe data use, through identifying the concept of "responsible use of data".

It states that – "*in this strategy, we use 'responsible data' to mean data that is handled in a way that is lawful, secure, fair, ethical, sustainable and accountable, while also supporting innovation and research.*" Additionally, the UK has also been undertaking pilots of the 'data trustees' framework, which also finds its mention in the national data strategy and the UK AI sector deal.[30]

A report on the lessons learned from the pilot has already been prepared and the strategy states that the relevant centres will continue to work on such models. This indicates that data trusts are a new model, and there are dimensions in their functionality that may need to be explored further based on existing institutional and demographic capacity.

Along with this, the learning from the pilots also suggest that data trustees should not dictate data sharing for 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 (that is, cannot be a judge in your own cause).[31]

Recommendations

Considering the context of the issues emerging out of the data governance framework as proposed by the CoE and contextualising it with the evolution of frameworks in other countries, the following recommendations should be considered to address these challenges highlighted in the key assessment above:

FIGURE 5: KEY RECOMMENDATIONS FROM A CONSUMER PERSPECTIVE

1. Clear Identification of Intended Beneficiary

The vague interpretations around "public interest" should be avoided and there should be clear identification of the targeted beneficiaries and the purpose of sharing such that a proper balance could be maintained between the community and individual interest in data.[32]

Some inspiration in this regard may be taken from the "rights-based approach" of the European frameworks, which while identifying the value in making data accessible has also given importance to the granularity of consent of data principals. This keeps the consumers at the core of such frameworks. At the same time, the mechanisms or methods, through which consent choices are being delivered to the consumers should be sensitive towards the capacity of the demography. Mechanisms, such as privacy labels might also help remove information asymmetry for consumers, encouraging them to make an informed choice.

The Australian Framework prescribes for purpose limitation to maintain proportionality and necessity in the usage of data, which is intended to ensure accountability and transparency in data usage and sharing. Overall, the analysis of comparative jurisdiction and other experiences with data access indicates that building of institutional, state and infrastructural capacity; and attaining a certain level of policy evolution in protecting the rights of data principals should be the building blocks of data sharing.

Along with the existing scrutiny of existing power-dynamics and data sharing framework should be designed in a way that it has various points and levels where consumers can contest decisions. In this regard, the most recent report of World Bank on 'Data for Better Lives' identifies that connecting the poor to the benefits of the data is important and to do so a new social contract with 'trust' at its core needs to be formulated. Furthermore, it suggested that for connecting the poor to the benefits of the data, well-crafted stated support to bridge demand and supply gaps, increasing digital literacy and upgrading technological infrastructure is vital.[33]

2. Consumer Empowering Privacy Architecture

It is essential to have strong data protection and privacy laws in place, before prescribing data-sharing frameworks. A similar trend is also being observed in the comparative jurisdiction indicated above, which already have data protection laws and require compliance with data protection principles in their subsequent data sharing strategy.

This policy sequencing in India would be crucial as many aspects of the application of the data protection principle could become clear informing and could inform subsequent data-sharing frameworks better. This could include consumer interaction with intermediates such as consent managers, awareness regarding data harms and industry capacity in segregating data. Additionally, it is important to recognise that privacy and security are not binaries and a balance between both needs to be sought after.

Additionally, creating binaries between personal and NPD is difficult and rather the focus should be on streamlining various data governance frameworks such as DEPA, National Health Data Management Policy, or the National AI strategy to prescribe a comprehensive strategy that can empower consumers to exercise their privacy rights through uniform consent architectures.

In this regard, inspiration may also be taken from the EU data strategy, as it proposes that the consumers or data subjects should be aware of how their data is being used and they should have granular control of their data. This approach stems from the strategies that aim to create a balance so that consumers can be empowered while facilitating data access. In this regard, DEPA has taken a step forward in this direction, however, the introduction of a consent dashboard needs to be evaluated, along with its potential harms, which have not been assessed in DEPA or other proposed data policies in India.


Needless to say, that various jurisdictions are experimenting with various data governance models, however, the Indian policy should aim for data governance policy to evolve with the consumer at its centre and considering its social-economic realities.

3. Standardisation of Anonymisation Technique

The core technical architecture, which the Report relies on is anonymisation and it puts far-reaching faith in its application. There is a need to re-work the anonymisation standards to stipulate the minimum technical marks that any method of anonymisation should meet to avoid differing privacy risks in datasets. These technical marks or standards should also be updated at regular intervals with the technology change. For this, more nuanced consultation would be required with experts who can inform the CoE about anonymisation techniques and industrial capacity to adopt such mechanisms. This would give more security for consumers' data.

4. Adopting Innovating Frameworks

To ensure that transparency and accountability are maintained throughout the data sharing chain appropriate principles of governance should be prescribed. Till now, the UK has been a pioneer in its work around data trusts and they have undertaken pilots to understand the functioning of such intermediaries. The lessons from the pilots conducted in the UK observed that it is necessary to clearly define data trusts and it may be challenging for them to protect the privacy and legal interest of the community and consumers.[34]

Along with this, it was also highlighted that data trust must avoid bias and maintain neutrality, for example, not using data for any associated for-profit purposes, which involves data trustees, and to ensure for data trustees to have independent funding. The reference of data trusts also finds its mention in the National UK Data Strategy and the UK AI Sector Deal with establishing sector-wise data trusts, depending on the potential and maturity of the sectors, however, this framework is at the experimentation stage at best.

Thus, drawing learning from the pilots of the UK, it might be beneficial that the application of such data trusts is first piloted in the Indian context, perhaps for sectors that are at more advanced stages of data management such as finance and also explore it as a regulatory sandbox model, based on the requirement of the markets and Indian context. It may also be beneficial to identify "trust" and "responsible data sharing principles", which have also been

recognised by both Singapore and the UK, to identify standards and mechanisms for ensuring fairness, accountability, integrity to inculcate greater trust of individuals in these intermediaries and the government, which are specific for the Indian context. For this, audit mechanisms and self-assessment tools could also be developed.

Learnings from different kinds of models can be taken to find the appropriate fit in the Indian context. While rights-based models of data governance have been seen as the benchmark in several of these jurisdictions, the nuances of the Indian jurisdiction call for a harm-based model. Such a model can be implemented with specific useful elements from other models, as such a model focuses on potential harms arising by a data request, with multiple layers of protection to risks and harms. [35]

Another alternative presented by scholarship is to take a bottom-up approach in establishing data trusts. Under this approach, it is suggested that consumers should be free to choose data trusts they want to represent by depending upon the principle of data sharing and accountability they offer. Through this, an appropriate balance could be made between consumers' choice and the flexibility required in the data economy.[36]

5. Addressing Collective Harms

Harms accruing from big data in the age of Artificial Intelligence (AI) and Machine Learning are difficult to predict, specifically how it may lead to collective harm for specific communities. This requires 'fighting AI with AI' through developing innovative technologies that can identify profiling, reputation or cybersecurity harms in big datasets, so that it becomes easier for the consumers to request such assessment.[37]

At the same time, it would also be beneficial to have a "risk-based approach" in data sharing as has also been stipulated within the Singaporean data-sharing framework, which proposes for developing a risk matrix for differing datasets and regularly conduct risk audits to update this matrix to keep pace with technological development.[38] This could help consumers identify harms that may emerge for them.

Additionally, it is equally important for consumers to have a simple and easily accessible grievance redress mechanism through websites or portals where they can register their complaints. It may also be helpful to explore alternative avenues for grievance redressal such as through setting up Consumer Service Cells by the data trustees on the lines of CUTS Grahak Sahayta Kendras,[39] Graamvani, Haqdarshak, which could act as mediator or conciliator in resolving the complaints.

6. Transparency in the Regulatory Process

It would be beneficial to create greater trust and transparency in the regulatory process, this was also highlighted by the UK National Data Strategy, which states that it is important to develop public trust in the systems of data governance. This could be done by ensuring greater

representation of consumer rights and civil society organisation in the design and management of the NPDA. Consultative processes where regular engagement with stakeholders is sought after in order to identify the problems first and then coming up with solutions to balance consumer interest, market growth and security.[40]

There could also be a provision for releasing transparency reports and details regarding the requests adjudicated to maintain accountability, along with robust checks and balances. Furthermore, there should be clear guidelines for consumers so that they can identify which regulator would be best suited to address their complaints.

Along with this, appropriate safeguards of purpose limitations and principles of proportionality, legality, and necessity as enshrined by the Supreme Court in the case *K.S Puttaswamy vs. Union of India*,[41] should be incorporated in all data governance policies.

Endnotes

1 https://static.mygov.in/rest/s3fs-public/mygov_160922880751553221.pdf

2 Jane Johnston, "Whose Interests? Why Defining the 'public Interest' Is Such a Challenge," *The Conversation*, 2017, http://theconversation.com/whose-interests-why-defining-the-public-interest-is-such-a-challenge-84278.

3 Barbara Prainsack, "Logged out: Ownership, Exclusion and Public Value in the Digital Data and Information Commons," *Big Data & Society* 6, no. 1 (January 1, 2019): 2053951719829773, doi:10.1177/2053951719829773.

4 Prashant Reddy, "Aadhaar: Amid the Debate about Privacy, the More Pressing Issue of Exclusion Has Been Forgotten," Text, *Scroll.In* (https://scroll.in, 2017), https://scroll.in/article/833080/aadhaar-amid-the-hullabaloo-about-privacy-the-more-pressing-issue-of-exclusion-has-been-forgotten.

5 Srikanth Lakshmanan. CUTS Webinar on the Future of Data Governance in India: A Consumer Perspective. March 12, 2021. Accessible at https://youtu.be/SK8BY7vEixc

6 Linnet Taylor. CUTS Webinar on the Future of Data Governance in India: A Consumer Perspective. March 12, 2021. Accessible at https://youtu.be/SK8BY7vEixc

7 Linnet Taylor and Luciano Floridi, 'Group Privacy: New Challenges of Data Technologies', *Group Privacy*, 2017, 293.

8 ECLI:EU:C:2017:994, para. 35

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/ and https://cuts-ccier.org/pdf/survey_analysis-dataprivacy.pdf

10 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

11 https://www.theguardian.com/technology/2019/jul/23/anonymised-data-never-be-anonymous-enough-study-finds,

12 https://theprint.in/opinion/india-has-to-toe-a-fine-line-in-defining-non-personal-data-between-public-interest-and-ipr/382149/

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

[14] 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

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

[16] Raghavan and Singh, "Building Safe Consumer Data Infrastructure in India: Account Aggregators in the Financial Sector (Part–2)," Dvara Research Blog(blog), accessed on February 04, 2020, https://www.dvara.com/blog/2020/01/07/building-safe-consumer-data-infrastructure-in-india-account-aggregators-in-the-financial-sector-part-2/

[17] Exclusion through which adequate representation is not give to certain demographics to be part of governance process. Barbara Prainsack, 'Logged out: Ownership, Exclusion and Public Value in the Digital Data and Information Commons', *Big Data & Society* 6, no. 1 (1 January 2019): 2053951719829773, https://doi.org/10.1177/2053951719829773.

[18] Aisling McMahon, Alena Buyx, and Barbara Prainsack, "Big Data Governance Needs More Collective Responsibility: The Role of Harm Mitigation in the Governance of Data Use in Medicine and Beyond," *Medical Law Review* 28, no. 1 (February 1, 2020): 155–82, doi:10.1093/medlaw/fwz016.

[19] https://cuts-ccier.org/pdf/policy-brief-grievance-redress.pdf

[20] Page 20, https://static.mygov.in/rest/s3fs-public/mygov_160922880751553221.pdf

[21] https://cuts-ccier.org/cdpp/ and https://cuts-ccier.org/pdf/survey_analysis-dataprivacy.pdf

[22] MeitY, Government of India, 2021. Accessible at https://www.meity.gov.in/writereaddata/files/Intermediary_Guidelines_and_Digital_Media_Ethics_Code_Rules-2021.pdf

[23] The Personal Data Protection Bill 2019. Available at: http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

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

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

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

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

[28] https://www.oaic.gov.au/privacy/australian-privacy-principles/

[29] https://www.gov.uk/government/publications/algorithms-how-they-can-reduce-competition-and-harm-consumers/algorithms-how-they-can-reduce-competition-and-harm-consumers

[30] https://www.gov.uk/government/publications/artificial-intelligence-sector-deal/ai-sector-deal

[31] https://docs.google.com/document/d/118RqyUAWP3WIyyCO4iLUT3oOobnYJGibEhspr2v87jg/edit#

[32] Srikanth Lakshmanan. CUTS Webinar on the Future of Data Governance in India: A Consumer Perspective. March 12, 2021. Accessible at https://youtu.be/SK8BY7vEixc

[33] https://www.worldbank.org/en/publication/wdr2021

[34] https://docs.google.com/document/d/118RqyUAWP3WIyyCO4iLUT3oOobnYJGibEhspr2v87jg/edit

[35] Amar Patnaik. CUTS Webinar on the Future of Data Governance in India: A Consumer Perspective. March 12, 2021. Accessible at https://youtu.be/SK8BY7vEixc

[36] Delacroix, S., & Lawrence, N. D. (2019). Bottom-up data Trusts: disturbing the 'one size fits all 'approach to data governance. *International data privacy law*, *9*(4), 236-252.

[37] 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. 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,

[38] Singapore Trusted Data Sharing Framework, 2019. https://www.imda.gov.sg/-/media/Imda/Files/Programme/AI-Data-Innovation/Trusted-Data-Sharing-Framework.pdf

[39] Consumer Care Centre (Grahak Sahayta Kendra) | CUTS Centre for Consumer Action, Research & Training (CART)," https://cutscart.org/consumer-care-centre-grahaksahayta-kendra/

[40] Amlan Mohanty and Nehaa Chaudhari. CUTS Webinar on the Future of Data Governance in India: A Consumer Perspective. March 12, 2021. Accessible at https://youtu.be/SK8BY7vEixc

[41] 2017 10 SCC 1