# Data Stewardship for Non-Personal Data in India

## A Position Paper on Data Trusts

### Collaborators

Vidhi Centre for Legal Policy

Indraprastha Institute of Information Technology, Delhi

Cyril Amarchand Mangaldas

Omidyar Network India

# About the Authors

Trishi Jindal and Aniruddh Nigam are Project Fellow and Research Fellow, respectively, at the Centre for Applied Law and Technology Research at the Vidhi Centre for Legal Policy, New Delhi.

The Authors would like to thank the following collaborators for their guidance and feedback in the preparation of this position paper: Ms. Akriti Gaur and Mr. Ameen Jauhar at the Vidhi Centre for Legal Policy, Mr. Sushant Kumar at Omidyar Network India, Mr. Pravesh Biyani at IIIT-Delhi and Mr. Amartya Roy, Ms. Richa Roy and Ms. Srishti Aishwarya at Cyril Amarchand Mangaldas.

The Authors would also like to thank Prof (Dr.) Shivprasad Swaminathan, Prof. Sudhanshu Kumar, Ms. Shehnaz Ahmed and Mr. Prashant Reddy for their insight on issues in this position paper.

This position paper has been prepared with the assistance of views solicited from participants at the stakeholder consultation meetings held on March 6, 2020 and August 7, 2020. The Authors would like to thank the participants at these meetings for their time and feedback.

Any errors or inaccuracies are the Authors' alone.

# Executive Summary

- Vast amounts of non-personal data are generated in the digital economy. However, there is a lack of institutional mechanisms which enable accessible and trusted sharing of such data. Existing models of data governance have failed to create an environment where the value generated from this data is distributed widely. Particularly, institutional arrangements of the digital economy do not appear to recognise the collective agency and interests of the larger community.

- This position paper develops the concept of 'data trusts' as a legal institution which can be used for the pooling, sharing and collective management of non-personal data. The phrase 'data trusts' has been used to describe arrangements where data is placed under the control of an entity which is under a fiduciary obligation to a set of beneficiaries – which could be the broader community, local populations or private entities. While there has been a lot of recent interest in the idea of data trusts, there is a lack of an established meaning, structure or understanding of this concept.

- This position paper provides institutional detail to the idea of a 'data trust'. Particularly in the context of non-personal data, it envisages of data trusts as participative institutions which can foster trusted exchange in non-personal data and reinstate the role of the community in this exchange.

- Data trusts, as described in this paper, would be specialised institutions which are bound by a legally enforceable fiduciary duty to advance the interests of the community. These institutions can operate as stewards of non-personal data and have a representative executive body. Their obligations and accountability should include meaningful transparency and consultation requirements, including at the local and sub-local level. The position paper envisages a competitive ecosystem of data trusts which intermediate and enable access to non-personal data, particularly to public and community non-personal data. This framework is intended to develop institutional mechanisms in the digital economy which promote an accessible market for non-personal data while safeguarding collective agency and interests of communities.

- This paper finds that existing statutory frameworks of operationalising non-profit entities do not offer a model which can help operationalise data trusts in an optimal form. To this end, it recommends a regulatory framework to bridge this policy gap and help make data trusts a reality. This is supplemented with efforts at establishing pilot data trusts to gain practical learnings and insights on the issue.

- Chapter I explores the need for a data governance solution for non-personal data. It examines the theoretical and material reasons for adopting a commons-based approach to the governance of non-personal data. It proposes that data stewardship can offer a solution which enables polycentric governance of non-personal data.

- Chapter II frames the key design principles which should be adopted in developing a commons-based framework for data stewardship. It assesses different models of data stewardship along these design principles and identifies data trusts as an attractive framework for developing participative models of data stewardship.

- Chapter III examines the ways in which a data trust can be operationalised within existing legal frameworks and trust law. It looks at existing models of operationalising non-profit entities and finds that existing statutory frameworks are inadequate at creating an organisational framework which satisfies the design principles identified in this paper.

- Chapter IV recommends a regulatory framework which can enable the operationalisation of data trusts. It develops this framework along the lines of the design principles identified in this paper and identifies several governance mechanisms – such as localised consultations and federated sub-committees – which can help the data trust recognise the role of the community. This chapter attempts to give shape and form to the concept of a data trust, as well as to the regulatory structure which can enable the development of data trusts in practice.

# Table of Contents

# Chapter I:

# A data governance solution for non-personal data

## Introduction

Questions of data governance increasingly occupy a prominent role in conversations related to the digital economy. With the increasing digitisation of various aspects of modern life, the data generated in various economic activities assumes great relevance not just to questions of the digital economy, but also the interests of individuals and communities. Access to data and control over data is likely to "*determine the economic positioning, independence and returns*" of various actors in their economic relations.[1] This prompts the need for an examination of the institutional mechanisms of data governance which structure these relationships.

The Report of the Committee of Experts on Non-Personal Data ("**NPD committee report**" or "**Report**") initiated a discussion around the concept of non-personal data, the rights of individuals and communities in relation to such data and the institutional frameworks which govern the ownership and use of such data in India.[2] Non-personal data ('**NPD**') is defined by the NPD committee report as data which does not contain any personally identifiable information. This includes data regarding weather conditions, data related to public transit systems, and in some instances, aggregated and anonymised data. The Report recommends three categories of NPD: public NPD, private NPD and community NPD. The Report makes recommendations aimed at promoting wide sharing of NPD. This policy direction indicates the need to examine institutional mechanisms which can enable such sharing at scale, safeguard the interests of the community and enable trusted exchange in NPD.

It is important to narrowly frame the problem that this paper attempts to address: while there may be substantial amounts of NPD which is collected and generated in the digital economy, there is a lack of institutional mechanisms for the sharing of such data to enable its usage by a broader set of users.[3] The consequence of this is a loss of the gains that could be obtained in an ecosystem where this data is widely shared. This is especially true for public NPD and community NPD. In the case of private NPD, the institutional make-up of the digital economy is oriented towards this data being collected by private companies or public agencies but it does not establish mechanisms through which they can share this data in a trusted manner, or are incentivised to do so. Therefore, holistically, despite the existence of several policies in this field, such as the National Data Sharing and Accessibility Policy 2012[4], an environment where NPD is widely shared has failed to materialise. This paper posits that the development of appropriate institutional mechanisms which enable trusted sharing and exchange of NPD can offer a way to allow for greater sharing of NPD, while balancing the interests of the various stakeholders involved such as data providers, data users and the communities related to NPD.

These institutional mechanisms can operate in many ways: they can aggregate public NPD and community NPD from open sources and make it

[1] Parminder Jeet Singh and Jai Vipra, 'Economic rights over data: A framework for community data ownership' DEVELOPMENT (2019)

[2] Report of the Committee of Experts on Non-Personal Data, Ministry of Electronics and Information Technology (2020)

[3] Charles Jones and Christopher Tonnetti, 'Nonrivalry and the economics of data' 110(9), American Economic Review (2020)

[4] National Data Sharing and Accessibility Policy, 2012, available at <https://nsdiindia.gov.in/nsdi/nsdiportal/meetings/NDSAP-30Jan2012.pdf>;

accessible to end-users; they can be custodians of data under mandatory data sharing policies, as envisaged in the NPD committee report, as well as in developments in the European Union; and they can procure NPD from private or public entities and make it available to end-users for societally beneficial purposes and on terms which are aligned to the interest of the larger community.

This paper posits that developing 'data trusts' – an institutional stewardship framework to govern the storage and sharing of NPD – can advance a participative and efficient mechanism to balance interests of stakeholders related to NPD. Data trusts, as formulated in this paper, provide an institutional structure for governing NPD as a commons resource.[5] The concept of data trusts, which is a relatively nascent concept, must also be tested in practice. This requires many different formulations – such as data stores, bottom-up data trusts, knowledge commons and trusted intermediaries – to be assessed on practical and operational metrics.

This position paper develops a model for data trusts along the lines of a 'civic data trust'. This implies the creation of a governance structure for entities which can act as responsible and efficient stewards of NPD. It envisages a competitive ecosystem of data trusts which intermediate access to community NPD. These data trusts may aggregate open data, procure data commercially or be recipients of data under data sharing policies. NPD can be made available by data trusts to end-users through license agreements and other contractual arrangements. These entities are participatively governed and are legally required to act in furtherance of a fiduciary obligation to the community. A competitive ecosystem of data trusts would give communities and end-users enhanced choice in terms of potential stewards for community NPD. While this conceptualisation of data trusts appears suitable in the context of NPD, other variants – such as 'bottom-up' data trusts, personal data stores and private data trusts – may be worthy of consideration in the context of personal data as well.

The research in this paper is supplemented by efforts in operationalising pilot data trusts to gain practical learnings and insight. Pilot projects which are implemented for specific regions and sectors – such as a pilot data trust for urban mobility data for a district– can offer a proof-of-concept for the ideas explored in this paper. Outputs from these pilots can offer instructive lessons for the lifecycles of different concepts of data trusts, which may be explored as part of continued research on this area.

**Chapter I** of this paper analyses the need for a commons-based solution for the governance of NPD. **Chapter II** posits that a stewardship-based framework can help structure such commons and analyses stewardship-based frameworks based on their alignment with the design principles for a 'knowledge commons'. **Chapter III** examines data trusts, which emerge as a suitable stewardship-based framework, from an operational perspective in the existing legal landscape. This exercise reveals the need for legislative and policy changes to make data trusts a reality, which are outlined in **Chapter IV**.

[5] Natalie Chyi and Yuliya Panfil, 'A Commons Approach to Smart City Data Governance: How Elinor Ostrom Can Make Cities Smarter' (2020), available at <https://www.newamerica.org/future-property-rights/reports/can-elinor-ostrom-make-cities-smarter/principle-4-promote-responsibility-for-data-governance-among-multiple-layers-of-nested-enterprises> Accessed 24 June 2020; 'Data Trusts: Lessons from three Pilots', Open Data Institute (2019), available at <https://docs.google.com/document/d/118RqyUAWP3WIyyCO4iLUT3oOobnYJGibEhspr2v87jg/edit#heading=h.3fngvdcfo2cs> Accessed 8 October 2020.

# The context of the digital economy

Conversations around an economic framing of data have witnessed a spectrum of disagreement about how data should be characterised. A traditional view posits that data should be characterised as a "resource" to be privately owned, like other forms of property. A slightly different view proposes that data, especially NPD, may be thought of as a resource which should be shared freely with minimal constraints.[6] This view has altruistic objectives, but it appears to ignore some of the economic implications of the market which it gives rise to. Physical and financial constraints limit the ability of many entities to collect data at scale, and the "*inequality of arms*" problem in data collection translates to concentration in the market for this resource.[7] On the other hand, some argue that framing data as a 'resource' undermines individual rights in relation to such data and invisibilises the role of human bodies in the creation of data.[8] Arguably, the above-mentioned positions undermine the effect that concentration of data has from the perspective of economic justice. Completely rejecting the resource-oriented conception of data undermines the effect data aggregation has on shaping digital markets and monopolies. It further entrenches a status quo which currently excludes individuals and communities from sharing the benefits emanating from the data. Therefore, while the reinstatement of human agency and community interests in data governance is key, this exercise must still engage with the aspects of data which give rise to its conceptualisation as a "resource" and the economic consequences thereof.

Data is not merely information – but serves to formulate digital intelligence, which refers to the insights provided by sophisticated analytics based on large sets of data.[9] This digital intelligence provides an entity with the ability to make better decisions that suit its economic interests, and provides them with the capability to predict, control and influence decision making by individuals.[10] Many successful digital companies have realised this value and accelerated processes for the aggregation of this data.[11] As the value of the digital intelligence which can be generated from data increases based on the amount of data being analysed, some argue that these companies have moved towards the establishment of "data enclosures", concentrating digital intelligence in the hands of a few companies.[12]

This issue pervades various sectors of the digital economy – ranging from online retail and transportation systems to social media platforms. The concentration of digital intelligence in a few successful digital companies leads to these insights being used primarily in pursuit of the economic interests of these companies. This may often not factor in the impact on communities and individuals.[13] The interests of communities – in terms of their economic interests and interests related to "group privacy" – stand to be ignored within the structural logic of existing arrangements of data governance. To reinstate the agency of the community, it is important to develop institutional mechanisms which recognise the role of the community in the generation of digital intelligence. The sharing of public and community NPD is a necessary first step in this process. In the instance of private NPD, institutional measures which incentivise sharing of NPD in a responsible and trusted manner may help reorient the digital economy to the public good. This is in addition to the necessary reinvigoration of traditional legal

[6] European Commission Staff working Document, on 'The free flow of data and emerging issues of the European data economy' (2017)

[7] Ostrom, E., R. Garder, and J. Walker, Rules, Games, and Common-Pool Resources, Michigan, The University of Michigan Press (1994)

[8] Anja Kovacs and Nayantara Ranganathan, 'Data sovereignty, of whom? Limits and suitability of sovereignty frameworks for data in India', Data Governance Network Working Paper 03 (2019)

[9] Parminder Jeet Singh, 'Data and Digital Intelligence Commons (Making a case for their community ownership)', Data Governance Network Working Paper No 02 (2019)

[10] Parminder Jeet Singh, 'Data and Digital Intelligence Commons (Making a case for their community ownership)', Data Governance Network Working Paper No 02 (2019)

[11] UNCTAD (2019). Value Creation and Capture: Implications for Developing Countries. Digital Economy Report 2019. UNCTAD.

[12] Parminder Jeet Singh, 'Data and Digital Intelligence Commons (Making a case for their community ownership)', Data Governance Network Working Paper No 02 (2019)

[13] Parminder Jeet Singh and Jai Vipra, 'Economic rights over data: A framework for community data ownership' DEVELOPMENT (2019)

frameworks, such as competition law, to address some of the issues discussed in this paper.

The community's role in the generation of digital intelligence is significant. Data of various kinds, such as transit data, is generated through the participation of individuals in a community. For example, Uber's intelligent transportation networks are built based on the data of drivers who participate in these systems and the individuals who avail these services.[14] However, this data is not made available or shared widely. As a consequence, while Uber is able to improve its transportation networks and pricing mechanisms, this data is walled off from uses which may be in the interests of the community such as developing sustainable transport solutions or improving urban planning. Similarly, small businesses on large e-commerce platforms like Amazon are increasingly finding that their business models are replicated by the platform, which based on its access to their data, is able to make decisions which further its economic incentives.[15] In many other cases, such as the collection of data through publicly funded sensors and systems, the establishment of basic conditions for the generation of digital intelligence are the result of infrastructure established by the state. The ability to operate a data extractive business is the result of various privileges afforded by the state to operate in a particular manner – however, the value generated by such businesses is concentrated to serve the interests of a few companies, undermining the interests of the community which creates the conditions for them to exist.

The process of navigating the digital economy must also recognise the necessity of maintaining incentives for individuals to participate in data intensive businesses. Addressing these varied interests requires the development of data governance solutions which can offer a polycentric solution to resolving these issues. While the exact contours of community rights over data are difficult to precisely draw out, a data governance solution which is mindful of these interests can help develop an environment where the benefits of digital intelligence flow to the broader community. The political economy of data governance must be examined from the perspective of institutional arrangements which structure economic relationships in the digital economy. This position paper examines institutional mechanisms which can reinstate the role of the community in the generation of value from data – thereby enabling data to be used for purposes which serve the interests of the community.

To this end, this chapter examines the economic framing of data as a resource and focuses on why it is necessary that a data governance solution should incorporate community interests in NPD. It proceeds to examine the different interests of the community in the economic systems surrounding NPD and identifies mechanisms through which these interests have been exercised. Finally, it examines how a stewardship model – in the form of a commons approach – can build the institutional arrangements needed to reorient the digital economy to achieve the public good.

[14] Dan Ciuriak and Maria Ptashkina, Leveraging the Digital Transformation for Development: A Global South Strategy for the Data-driven Economy, CIGI Policy Brief No 148 (2019)

[15] Lina Khan, Amazon's Antitrust Paradox, 126 Yale Law Review (2016)

# The case for polycentric governance of NPD

The collection and processing of NPD has largely functioned in the absence of a governance framework – across jurisdictions, there is often no specific framework which governs how NPD may be collected or processed. Legal frameworks have operated to recognise certain ownership or propertarian rights in relation to NPD, either recognising traditional propertarian-rights over NPD[16] (for example, the collector of NPD owns the data as their property) or through other frameworks such as intellectual property rights[17] (for example, the database-right in the European Union), or by recognising confidentiality interests or trade secrets in data.[18]

However, as the processes of digitisation have expanded into several more *traditional* sectors – such as transportation, urban planning and agriculture – the value of non-personal data has come to the fore, and the lack of a sophisticated governance framework for NPD has become relevant to questions of how the digital economy is shaped.[19] Further, the polycentric nature of NPD has also become a significant part of the academic discussion on this issue, challenging the traditional view of "ownership" of NPD by the collector.[20]

Some scholars have referred to the concentration of NPD as the key factor which enables a company to act as the "brain" of the business ecosystem they inhabit.[21] As per this scholarship, successful digital companies occupy a critical position in the digital economy by virtue of the large amount of data possessed by them. This data, coupled with sophisticated analytical systems, allows them to generate advanced predictions and insights which drive decision-making – thereby enabling an advantage in the digital economy.[22] There are various sectors where this concentration of digital intelligence can yield powerful insights for a company – whether it is in supply chain management, organising transportation networks, coordinating prices or managing task allocation. Companies like Amazon, Uber, Google and Facebook have demonstrated significant concentration of digital intelligence in their respective sectors – which has enabled them to entrench a near-dominant market position in many of these sectors.[23] The development of an environment which enables wide and trusted sharing of NPD can help distribute the benefits of the generation of digital intelligence.

As the digital economy grows, it is key that digital intelligence – which is a valuable resource in terms of decision-making – is not allowed to be concentrated amongst a handful of entities. Particularly, if there are institutional designs which can prevent this concentration and create an accessible market for the sharing of NPD, then they are worthy of detailed inquiry. To this end, this part looks at some of the interests that the community has in NPD, especially in respect of aggregate NPD. Once these interests are identified, this chapter examines some of the mechanisms traditionally used to exercise control over NPD and finds that these are insufficient in recognising the role of the community in relation to NPD. Finally, it is argued that a stewardship solution – drawing from literature on 'knowledge commons' – may be best placed to reinstate the role of the community in the political economy of the governance of NPD.

[16] *See* Herbert Zech, 'A legal framework for data economy in the European Digital Single Market: rights to use data', 11(6), Journal of Intellectual Property Law and Practice, 460 (2016)

[17] Josef Drexl, 'Designing competitive markets for industrial data: Between propertisation and access', JIPITEC 257 (2017)

[18] Tanya Aplin *et al*, 'Gurry on breach of confidence' (1984)

[19] Josef Drexl, 'Designing competitive markets for industrial data: Between propertisation and access', JIPITEC 257 (2017)

[20] Parminder Jeet Singh, 'Data and Digital Intelligence Commons (Making a case for their community ownership)', Data Governance Network Working Paper No 02 (2019)

[21] Gaurav Batra, Andrea Queirolo and Nick Santhanam, 'Artificial intelligence: The time to act is now', McKinsey (2018); Parminder Jeet Singh, 'Data and Digital Intelligence Commons (Making a case for their community ownership)', Data Governance Network Working Paper No 02 (2019)

[22] Parminder Jeet Singh, 'Data and Digital Intelligence Commons (Making a case for their community ownership)', Data Governance Network Working Paper No 02 (2019)

[23] Parminder Jeet Singh, 'Data and Digital Intelligence Commons (Making a case for their community ownership)', Data Governance Network Working Paper No 02 (2019)

# Framing community interests in NPD

## Conceptualising NPD as a 'common-pool' resource

A prominent narrative in the economic framing of NPD has been of data as an open access resource which can be collected by anyone. Legal systems which share this premise sometimes protect property-rights in this data by recognising the collector of NPD as its "owner".[24] Such an arrangement, where the underlying good is available to all, and legal protections to preserve property are secured by the State[25] resembles governance of "club goods", where legal recognition is granted to rules which exclude access to a resource in the control of another. While it is true that data can be collected by anyone, this notion obfuscates a deeper "inequality of arms" problem – where only a few organisations have the technical means to collect and process this data.[26] However, proponents of property interests in NPD claim that in the absence of rules which protect commercial interests in data, there may be a lack of incentives to collect data and run data-intensive businesses.

The traditional view of NPD rests on a thinking of data as a non-rivalrous good. This means that one individual's use of data does not prevent another from using that data.[27] The degree of excludability, that is, the degree to which another individual can be walled-off from such data depends on the level of technical investment and legal restrictions.

The argument in favour of the existing governance framework for NPD posits that NPD exists as a non-rivalrous good, and therefore, the concentration of NPD in the hands of the entity which collects it should not have a negative impact on other entities who can also collect it. An implication of this characterisation is that from a social perspective, it is desirable for non-rivalrous data to be widely shared so that many people may make use of it and broader social gains can be generated.[28] However, this outcome does not materialise because of the private incentives of companies which collect this data to avoid competition from other entrants and retain their incumbent advantage.[29] This leads to issues of concentration of data and undermines the benefits that could be achieved from wider sharing of data.

A key idea which may explain the failure of the emergence of an accessible market in NPD is that the resource in question is not data *simpliciter*, but the concept of digital intelligence.[30] This is to say that data becomes useful when it is embedded in systems which can collect enough amounts of data, analyse this data and offer insights based on this data.[31] The application of digital intelligence is also useful when it is applied to real world systems, such as an application that coordinates and provides services. These systems – including technical and physical systems – are socially situated, and not widely accessible.[32] For example, digital platforms, due to the presence of network effects, often tend towards a winner-takes-all market structure, and consequently, some scholars state that "*where a digital platform is dominant in a given sector, there is often little space for another one to develop, even if*

[24] Herbert Zech, 'A legal framework for data economy in the European Digital Single Market: rights to use data', 11(6), Journal of Intellectual Property Law and Practice, 460 (2016)

[25] Greg Bloom, 'Towards a community data commons', available at < https://beyondtransparency.org/chapters/part-5/towards-a-community-data-commons/> Accessed 12th October 2020

[26] Ostrom, E., R. Garder, and J. Walker, Rules, Games, and Common-Pool Resources, Michigan, The University of Michigan Press (1994)

[27] Charles Jones and Christopher Tonnetti, 'Nonrivalry and the economics of data' 110(9), American Economic Review (2020)

[28] Yan Carrierre Swallow and Vikram Haksar, 'The Economics and Implications of Data: An integrated perspective', International Monetary Fund Strategy, Policy and Review Department No 19/16 (2019)

[29] Charles Jones and Christopher Tonnetti, 'Nonrivalry and the economics of data' 110(9), American Economic Review (2020)

[30] Parminder Jeet Singh, 'Data and Digital Intelligence Commons (Making a case for their community ownership)', Data Governance Network Working Paper No 02 (2019)

[31] Parminder Jeet Singh, 'Data and Digital Intelligence Commons (Making a case for their community ownership)', Data Governance Network Working Paper No 02 (2019)

[32] Nadezhda Purtova, 'Health data for common good: Defining the boundaries and social dilemmas of data commons' in 'Under observation: The interplay between eHealth and surveillance' (Samantha Adams et al ed.) (2017)

*it had access to all the required data.*"[33] In this situation, the use of data by a digital platform – and the consequent walling-off of that data from the rest of the economy – has the effect of turning digital intelligence into a rivalrous good where once that data is collected by someone, it is difficult for someone else to have access to it.

Consequently, even though raw NPD by itself may be non-rivalrous, the formulation of digital intelligence – which is embedded in real world systems of collection and analysis of data and the provision of services – happens in a manner where if one person is able to formulate such digital intelligence, it ordinarily prevents another person from having such intelligence. This should prompt a recharacterization of NPD from an economic perspective.

This also points to the fact that it may be useful to think of NPD as a "common-pool resource" in several circumstances. This is particularly where the systems which provide economic utility to NPD are rivalrous and an "inequality of arms" problem persists. An implication of this is that the development of a commons governance framework for NPD may be desirable in those cases. Similar developments have been witnessed in the context of genomic data – which while earlier was perceived from an open access lens, and has slowly come to be governed by a commons regimes.[34] While not all kinds of NPD may be easily classifiable as a common-pool resource, the "inequality of arms" problem in respect of digital intelligence is arguably cross-sectoral.

The argument for thinking of a commons governance framework for NPD is sustained on the idea that where a resource is classified as a common-pool resource, the governance framework for that resource should be attuned to its nature. Where the governance framework recognises the true economic nature of the resource, it may lead to optimal allocation of benefits derived from that resource. The mismatch between the economic nature of NPD, as discussed above, and the current governance framework for NPD could arguably explain why the wide sharing of NPD has not materialised, despite raw data traditionally being considered non-rivalrous. The interests of the community, therefore, emerge primarily in ensuring that there is an optimal allocation of the benefits that may be derived from NPD.

## Economic rights of the community

The theoretical discussion about the economic nature of NPD invokes the material discussion about the interests of a community in NPD. As discussed previously, digital intelligence derived from NPD is generated through social processes.[35] These social processes, which are embedded within a community context, are key to the formulation of any NPD. While this digital intelligence, for example, in the case of mobility data could be used to develop public-centric applications and sustainable transport solutions, it is often used in a much more restricted manner by a successful private company. Additionally, the enclosure of important digital intelligence by a few enterprises to the exclusion of others works against the interests of the public, where local governments, civil society organisations, researchers and start-ups providing important public services do not have affordable or readily available access to important information.

All people, under the International Covenant on Economic, Social and Cultural Rights, have been granted the right to "*for their own ends, freely dispose of their natural wealth and resources*".[36] A similar imperative underlies the concept of the "public trust doctrine", which is also recognised in Indian law[37] – where some resources are deemed to be held by the State in trust for its people. This doctrine has often been invoked in the context of natural (as well as non-natural) resources to question State mismanagement of resources, or to deny rights of private ownership in respect of certain

[33] Parminder Jeet Singh, 'Data and Digital Intelligence Commons (Making a case for their community ownership)', Data Governance Network Working Paper No 02 (2019)

[34] Robert L Grossman, 'Data lakes, clouds and commons: A review of platforms for analyzing and sharing genomic data' 35(3) TRENDS IN GENETICS, 223 (2019)

[35] Parminder Jeet Singh, 'Data and Digital Intelligence Commons (Making a case for their community ownership)', Data Governance Network Working Paper No 02 (2019)

[36] Article 1.2, International Covenant on Economic, Social and Cultural Rights (1976)

[37] MC Mehta v Kamal Nath (1997) 1 SCC 388; MI Builders Pvt Ltd v Radhey Shyam Sahu, AIR 1999 SC 2468.

resources.[38] Notably, one of the key imperatives of this doctrine – that a resource should be utilised in the interests of the broader political community[39] – is significant in the context of NPD as well. Many of the resources which are within the ambit of the public trust doctrine – such as forests and water resources – have witnessed the establishment of commons governance frameworks to ensure sustainable, public-centric use of those resources.[40]

However, the structural logic of the digital economy does not require digital intelligence to be used for the ends of the community. In fact, existing arrangements are not oriented towards enabling many such uses of NPD,[41] which can arguably be characterised as the resources of a community. The monopolisation of various sectors of the digital economy, and the capture of digital intelligence in those sectors creates a need for a review of the institutions of the digital economy. Institutions which allow digital intelligence about a community to be used in ways that further the interests of that community should be the building blocks of this economy. A governance solution which grants the community with a say in determining how the material resources of that community are utilised is necessary to vindicate this right.

## The concept of group privacy

The NPD Committee Report also recognises the concept of "group privacy", which it defines as "*possibilities of collective harm related to Non-Personal Data about a group or community that may arise from inappropriate exposure or handling of such data*".[42] However, the precise boundaries of what amounts to group privacy are not made clear in the report.[43]

While privacy is generally conceptualised from an individualistic standpoint, there is a collective dimension of privacy which emerges in the context of aggregated data.[44] Modern techniques of data analytics are capable of identifying precise insights based on aggregate data. This also extends to identifying behavioural sub-groups,[45] or making inferences about the attributes of a particular sub-group,[46] that can have implications for that sub-group. For example, data about transportation behaviour relating to a pin-code, even where it involves no "personal" information, can be used to exploitatively design surge-pricing mechanisms.[47] In more significant instances where a lack of "group privacy" could lead to harm, such information could be used for discriminatory service provision or targeted violence.

While the discussion on group privacy is fairly nascent, it implicates the need for greater control by the community over data which relates to it.[48] Mechanisms which can help exercise this control can help mitigate some of the risks related to group privacy, by ensuring that the community has a say in how aggregate data about that community is used.

[38] Siddharth Manohar et al, 'Understanding data stewardship: taxonomy and use cases', AAPTI INSTITUTE (2020) <https://uploads.strikinglycdn.com/files/64aa4010-6c11-4d6f-8463-efaed964d7d9/Understanding%20Data%20Stewardship%20-%20Aapti%20Institute.pdf> accessed 14 April 2020.

[39] Lloyd R Cohen, 'The public trust doctrine: an economic perspective', 29 Cal WL Rev (1992)

[40] Sheila Foster and Christian Iaione, 'Ostrom in the City: Design Principles for the Urban Commons' (2017), available at < https://www.thenatureofcities.com/2017/08/20/ostrom-city-design-principles-urban-commons/> Accessed June 26, 2020.

[41] Parminder Jeet Singh, 'Data and Digital Intelligence Commons (Making a case for their community ownership)', Data Governance Network Working Paper No 02 (2019)

[42] Report of the Committee of Experts on Non-Personal Data, Ministry of Electronics and Information Technology (2020)

[43] Divij Joshi, 'Non personal data regulation: Interrogating group privacy', Centre for Law & Policy Research Blog, available at < https://clpr.org.in/blog/non-personal-data-regulation-interrogating-group-privacy/> Accessed 26th August, 2020

[44] Baar L Kammourieh *et al*, 'Group privacy in the age of big data' in 'Group Privacy: New Challenges of Data Technologies' (L. Taylor ed.) (2017)

[45] Brent Mittelstadt, 'From individual to group privacy in big data analytics' 30 Philosophy and Technology, 475 (2017)

[46] Brent Mittelstadt, 'From individual to group privacy in big data analytics' 30 Philosophy and Technology, 475 (2017)

[47] Salon Barocas and Helen Nissenbaum, 'Big Data's End Run around Anonymity and Consent' in Privacy, Big Data and the Public Good (Julia Lane et al ed.) (2014)

[48] Divij Joshi, 'Non personal data regulation: Interrogating group privacy', Centre for Law & Policy Research Blog, available at < https://clpr.org.in/blog/non-personal-data-regulation-interrogating-group-privacy/> Accessed 26th August, 2020.

# Evolution of mechanisms to exercise control over data

The concept of NPD has witnessed significant regulatory attention recently, but the legal mechanisms which exist to exercise control over data have been static. This section explores the evolution of these mechanisms to identify the need for a stewardship solution for exercising control over data at a community level.

## Property based controls over data

Property rights and ownership are an oft-cited means to exercise control over a resource.[49] Legally and politically, it means a right to a resource against everyone else (a right *in rem*) which is recognised by the government.[50] In the context of data, one mechanism for exercising control over its use and management emanates from its 'ownership'.[51] This is premised on the view that when data is collected, arranged or processed to yield digital intelligence, it is the result of human effort in choosing the data and employing the tools necessary to analyse the data.[52]

This would imply that the collector of data owns the data as it has chosen to invest in the means for data collection. As such, treating data as private property – whether in the context of individuals having ownership over personal data or data collectors having ownership over aggregation of personal and non-personal data – can set boundaries regarding its exclusive use and enjoyment of the value generated from it.[53]

## Shortcomings of an 'ownership' based perspective

An ownership based perspective fails to acknowledge that data is generated through a series of social processes.[54] The treatment of data as 'property' to be 'owned' by the collecting entity alienates the individual from this data, who plays a crucial role in generating this data and experiences the impact of any use of this data. To a limited extent, the recognition of privacy rights within the data help reinstate individual rights and control over data. These rights are not necessarily drawn from property and ownership-based claims. Instead, they have evolved from constitutionally protected liberty interests. This right is now enshrined within the Indian Constitution as a fundamental right.[55]

In the absence of privacy-based protections, the individual – who has undertaken the activity which led to the generation of the data, and the community – which has created the necessary conditions for the collection of the data, are alienated from control over this data. This alienation points to the inadequacy of "ownership" based controls in the context of NPD.

A second manner in which ownership operates is to create induced or manufactured scarcity of data.[56] Hess and Ostrom state that technologies can enable the "*capture of free and open public goods*"[57]. For instance, the rate of extraction of fish from a lake through a fishing rod is significantly lower than that where industrial fishing vessels are employed, and

[49] Herbert Zech, 'A legal framework for data economy in the European Digital Single Market: rights to use data', 11(6), Journal of Intellectual Property Law and Practice, 460 (2016)

[50] Black's law dictionary (6th ed) as discussed in para 19, Vikas Sales Corporation & Anr. v. Commissioner of Commercial Taxes (1996) 102 STC 106.

[51] Sylvie Delacroix and Neil D Lawrence, 'Bottom-up data Trusts: disturbing the 'one size fits all' approach to data governance', (2019) 9(4) International Data Privacy Law 236.

[52] Teresa Scassa, 'Data Ownership', CENTRE FOR INTERNATIONAL GOVERNANCE INNOVATION (2018) <https://www.cigionline.org/sites/default/files/documents/Paper%20no.187_2.pdf> Accessed 14 April, 2020; Arghya Sengupta, 'Why the Srikrishna Committee rejected ownership of data in favour of fiduciary duty', THE WIRE, 02 August 2018 <https://thewire.in/tech/why-the-srikrishna-committee-rejected-ownership-of-data-in-favour-of-fiduciary-duty> Accessed 13 April 2020

[53] Randy T. Simmons, 'Property and the Public Trust Doctrine' (2007) <https://www.perc.org/wp-content/uploads/old/ps39new.pdf> Accessed 14 April 2020.

[54] Peter Pels, Igor Boog et al, 'Data management in anthropology: the next phase in ethics governance?', https://onlinelibrary.wiley.com/doi/full/10.1111/1469-8676.12526.

[55] Justice KS Puttaswamy v Union of India (2017) 10 SCC 1.

[56] Peter Pels, Igor Boog et al, 'Data management in anthropology: the next phase in ethics governance?', https://onlinelibrary.wiley.com/doi/full/10.1111/1469-8676.12526.

can lead to overfishing, thereby creating rivalry for a resource previously characterised as a public good.[58] In the context of NPD, a sophisticated embedded system of data collection – such as a major digital platform engaged in service delivery – holds significant amounts of data and restricts the availability of data for the public or for other entities.[59] The "inequality of arms" problem, which was discussed previously, further compounds this artificial scarcity.

The legal issues with the concept of ownership over NPD are discussed in detail in the next chapter. However, it should be noted here that ownership is an imperfect formulation to capture the control that someone has over a resource.[60] This is further compounded in the case of data – where the rights implicated in data have a less definitive form than in more traditional examples of property.[61] As such, if 'ownership' is understood as a bundle of rights, then the particular rights in question must be specifically examined,[62] and the rubric of 'ownership' appears to lose its persuasive strength in more complex understandings of data.

## Reinstating community rights within data

The challenges associated with exclusive ownership of data can arguably be addressed in a limited manner through a number of alternative measures, such as through data sharing policies or compulsory licensing on fair reasonable and non-discriminatory (FRAND) terms.[63] However a truly 'polycentric conceptualisation' of data should allow diverse kinds of interests to be recognised in this data, as opposed to the much more simplistic notion of a single 'owner' of the data.[64] 'Polycentric governance' refers to a governance approach involving multiple, tangential jurisdictions, negotiating rules and policies to address common problems.[65]

As such, treating NPD as a resource in which the rights of the broader community subsist reinstates the role of the community in the value creation process related to data.[66] This argument has two legs: first, the value of a dataset increases owing to the network effects associated with it, and the community helps produce these network effects through participation within society.[67] Second, a significant portion of technology and NPD were created collectively, "*with the underlying infrastructure being created collectively through initial public investment in resources*".[68] This may

[57] CHARLOTTE HESS AND ELINOR OSTROM, Introduction: An Overview of the Knowledge Commons, UNDERSTANDING KNOWLEDGE AS A COMMONS: FROM THEORY TO PRACTICE, Pg 10., available at https://wtf.tw/ref/hess_ostrom_2007.pdf

[58] E. Ostrom, R. Garder, and J. Walker, 'Rules, Games, and Common-Pool Resources', Michigan, The University of Michigan Press, 1994 as cited in Nadezhda Purtova, *Health Data for Common Good: Defining the Boundaries and Social Dilemmas of Data Commons (July 9, 2016). in* RONALD LEENES, NADEZHDA PURTOVA, SAMANTHA ADAMS *(*EDS.*) (2017)* UNDER OBSERVATION - THE INTERPLAY BETWEEN EHEALTH AND SURVEILLANCE*, Springer; Tilburg Law School Research Paper No. 15/2016.* available at https://ssrn.com/abstract=2807455.

[59] National Academies of Sciences, Engineering, and Medicine, 'Data Sharing Guidance for Public Transit Agencies Now and in the Future', (2020) THE NATIONAL ACADEMIES PRESS 51, available at <https://doi.org/10.17226/25696> Accessed 25th August 2020.

[60] Patrik Hummel, Matthias Braun and Peter Dabrock, 'Own data? Ethical reflections on data ownership', Philosophy and Technology (2020)

[61] Yan Carrierre Swallow and Vikram Haksar, 'The Economics and Implications of Data: An integrated perspective', International Monetary Fund Strategy, Policy and Review Department No 19/16 (2019)

[62] Patrik Hummel, Matthias Braun and Peter Dabrock, 'Own data? Ethical reflections on data ownership', Philosophy and Technology (2020)

[63] Parminder Jeet Singh, 'Data and Digital Intelligence Commons (Making a Case for their Community Ownership)', available at <https://itforchange.net/sites/default/files/1673/Data-commons.pdf> Accessed 24 June 2020

[64] Elinor Ostrom, 'Beyond Markets and States: Polycentric Governance of Complex Economic Systems', (2010), 100(3) American Economic Review, 641.

[65] David Feldman, 'Polycentric Governance' in W.S. Bainbridge, M.C. Roco (eds.), 'Handbook of Science and Technology Convergence' at 877 (2016), available at <https://faculty.sites.uci.edu/feldman/files/2018/11/BC-3.pdf> Accessed 6 October, 2020.

[66] Stuart Mills, 'Who Owns the Future? Data Trusts, Data Commons, and the Future of Data Ownership', Future Economies Research and Policy Paper No. 7 (2020)

[67] Greg Bloom, 'Towards a community data commons' in Beyond transparency: Open data and the future of civic innovation' (Brett Goldstein and Lauren Dyson eds.) (2013), p.255.

[68] Mariana Mazzucato, 'Let's make private data into a public good', (2018) MIT Technology Review (2020.)

include public infrastructure such as roads, weather sensors, public transport networks as well as the underlying telecommunication infrastructure which enables the collection of the data.

Furthermore, protections for individuals recognised under personal data protection frameworks may not be strictly applicable to NPD. In the case of NPD, which may be collected at an aggregate level, and which may not identify an individual, the right to control the use of data may not vest with a single identifiable individual. At the same time, the community's interests in the data remain relevant as – (a) the information about one individual can yield behavioural insights for the wider community, (b) even if some individuals opt out of the sharing arrangement, their association with others within the same community can yield insights regarding them,[69] and (c) any harm or benefit accruing from the use of this data will likely flow back to the individual.[70]

The following example succinctly materialises the kind of twin concerns which must be balanced in any data governance solution for NPD: data collected by a town in the United States on flooding within their community in the form of maps, photographs of the flooding, etc. – which is all NPD collected with reference to the locality – helped them demonstrate their grievances regarding periodic flooding and hold their local administration accountable for faulty city planning. At the same time, the same data could also be used to increase mortgage and insurance prices for the community if shared openly without sufficient controls.[71]

In situations such as this, a governance solution which can exercise control over the manner in which the data is used would help safeguard the interests of the community in the development of digital intelligence. Recognising these twin concerns, discourse on the governance of common resources has emphasised a shift away from frameworks tied to ownership and individual privacy. Instead, it has advocated for solutions which would impose enforceable obligations to safeguard public (and the group's) interests when the resource is *used*, thereby enabling responsive and dynamic governance of NPD.

[69] Joshua A.T. Fairfield & Christoph Engel, 'Privacy as a Public Good', (2015) 65(3) Duke Law Journal, (2020).

[70] Parminder Jeet Singh, 'Data and Digital Intelligence Commons (Making a Case for their Community Ownership)', available at <https://itforchange.net/sites/default/files/1673/Data-commons.pdf> Accessed 24 June 2020.

[71] Richard Beckwith, John Sherry et al, 'Data Flow in the Smart City: Open Data Versus the Commons' (2018), available at <https://link.springer.com/chapter/10.1007/978-981-13-2694-3_11> Accessed 25 August 2020; Teresa Scassa, Designing Data Governance for Data Sharing: Lessons from Sidewalk Toronto (2020), 44–56, available at: https://doi.org/10.26116/techreg.2020.005

# Stewardship of data as a governance solution

Stewardship of a resource is an alternative form of governing a resource. Under stewardship, an overt obligation to ensure the public interest assumes paramount importance. Thus, common resources are managed by the State *"in trusteeship for the free and unimpeded use of the general public"*.[72] Even if the sovereign is permitted to own the resource, and grant property rights to private owners, such ownership cannot impede the public's rights in accessing these resources.[73] This *stewardship-based* understanding of common resources also extends to management of municipal resources, such as common parks, which are tied to the rights to "*light, air, privacy*" for local residents.[74] Even where municipal governments approve economic construction activities within a locality, they must act under an obligation to ensure that the rights of residents in a residential area are not ill-affected.[75]

Alongside the recognition of community interests by state actors, community-based models of governance are another key mechanism of managing common resources. Based on the work of Elinor Ostrom, a "commons" can be set up to pool and collectively manage community resources under a defined governance system.[76] Commons management frameworks have also, thereafter, been applied to "knowledge" to effectuate systems aiming to enable wider sharing of art, literature and research for the benefit of society. "Knowledge commons" have been developed as institutionalised frameworks that govern the sharing and creation of intellectual and cultural resources in accordance with shared values.[77]

"Data commons" are being developed globally to enable sharing of data, while protecting community and public interest.[78] These data commons can help safeguard user trust and autonomy by collectivising decision-making and empowering them to act together rather than alone.[79] These may be set up as a trusted intermediary that manages data for individual data sharing entities based on common standards that reflect the public interest.[80] We draw on these ideas of advancing public interests in NPD and enabling data sharing within an overarching framework that works towards the public interest to develop a data commons. The next chapter delves into the exact form of stewardship and the features that are necessary to conceptualise a data common(s).

[72] MC Mehta v Kamal Nath (1997) 1 SCC 388.

[73] Joseph L Sax, 'The Public Trust Doctrine in Natural Resource Law: Effective Judicial Intervention', (1970) 68 Michigan Law Review 471.

[74] Smt. Fatima Joao v Village Panchayat of Merces and Another 2001 (1) MhLj 836

[75] K. Ramdas Shenoy v Chief Officer, Town Municipal Council, Udipi 1974 AIR (SC) 2177.

[76] Elinor Ostrom, GOVERNING THE COMMONS (1990

[77] Brett Frischmann, Michael Madison et al, 'Governing Knowledge Commons', in Brett Frischmann, Michael Madison et al (eds.), *Governing Knowledge Commons* (Oxford University Press, 2014) 1 (Knowledge commons have been created for the pooling and creation of genome research, free information repositories like Wikipedia, collective creation of music through jam bands, etc. to enable trusted sharing of information and creative works, and enhancing the quality of public knowledge pool).

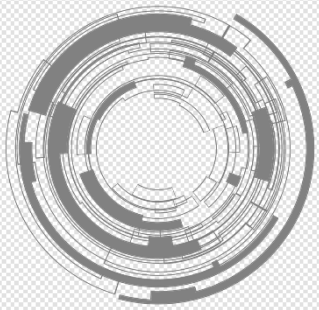
[78] Yuliya Panfil and Andrew Hagopian, 'A Commons Approach to Data Governance', (2019) New America Foundation, available at < https://www.newamerica.org/weekly/commons-approach-to-data-governance/> Accessed 25 August 2020.

[79] Barbara J Evans, 'Power to the People: Data Citizens in the Age of Precision Medicine', (2017) 19(2), Vanderbilt Journal of Entertainment and Technology Law 243; Janis Wong and Tristan Henderson, 'Co-Creating Autonomy: Group Data Protection and Individual Self-determination within a Data Commons', (2020) 15(1) International Journal of Digital Curation, 16.

[80] Siddharth Manohar et al, 'Understanding data stewardship: taxonomy and use cases', Aapti Institute (2020).

# Chapter II:

# Data trusts as an optimal stewardship model



## Stewardship of data and institutional innovation

In economic history, a key inquiry has been studying the emergence of businesses and markets, and the many factors that lead to the growth of different kinds of markets.[81] A significant portion of literature is dedicated to identifying the role that the emergence of new organisational forms plays in the growth of a market.[82] The premise of this view is that the organisational form of the firm is a key determinant of the functioning of an economy.[83] For example, studies demonstrate that the difference in industrialisation between north-western Europe and societies like Italy and Iberia can be explained, in part, by the emergence of formalised business organisations and accounting practices in north-western Europe as opposed to the more traditional guild dominated societies of Italy.[84]

Similarly, the joint-stock company has been hailed as an institutional innovation that transformed commerce. Over the sixteenth century, the increasing formalisation of businesses, better systems of maintaining records and development of new accounting systems allowed large enterprises to be better managed, leading to the emergence of the joint-stock company.[85] These firms had a better ability to operate at scale, and this enabled a broad-base of diffused investors to invest in large scale projects, which was a sharp contrast to the largely patronage-led or guild-based enterprises of the previous century.[86] Similarly, in Germany, the representation of banks on the supervisory board of joint-stock companies is an institutional innovation that is credited for mitigating information asymmetries between banks and lenders in the credit market.[87] Consequently, it is often credited for the health of the German credit system.[88]

This literature points to the critical role that the organisational form of the basic unit of the economy can play in its development. In the context of the emerging digital economy, it can be argued that the profit-oriented company is the basic unit of this economy. Literature on the platform economy posits "digital platforms" as this basic unit. [89] Despite the economic distinctions between traditional firms of the 20th century and modern digital platforms, the organisational form of the modern corporation has consistently been a core institution of the digital economy.

The prevalence of for-profit companies at the forefront of the digital economy might help explain some of the objectives towards which the economic system of the digital economy is oriented. The

[81] La Porta, Rafael, et al. "Law and finance." Journal of political economy 106.6 (1998): 1113-1155; La Porta, Rafael, et al. "Legal determinants of external finance." The journal of finance 52.3 (1997): 1131-1150.; Acemoglu, Darius and Johnson, B. "Unbundling institutions" Journal of Political Economy (2005).

[82] John F Padgett and Walter W Powell, 'The emergence of organization and markets' (2013)

[83] Ogilvie, Sheilagh. Institutions and European Trade: Merchant Guilds, 1000-1800 (2011).

[84] Ogilvie, Sheilagh. Institutions and European Trade: Merchant Guilds, 1000-1800 (2011).

[85] Kieser, Alfred. "Organizational, institutional, and societal evolution: Medieval craft guilds and the genesis of formal organizations." Administrative Science Quarterly (1989): 540-564

[86] Kieser, Alfred. "Organizational, institutional, and societal evolution: Medieval craft guilds and the genesis of formal organizations." Administrative Science Quarterly (1989): 540-564

[87] Jeremy Edwards and Sheilagh Ogilvie, 'Universal banks and German industrialisation: A reappraisal' 49(3) The Economic History Review (1996)

[88] Jeremy Edwards and Sheilagh Ogilvie, 'Universal banks and German industrialisation: A reappraisal' 49(3) The Economic History Review (1996); La Porta, Rafael, et al. "Law and finance." Journal of political economy 106.6 (1998)

[89] Bertin Martens, 'How online platforms challenge traditional views of the firm and the regulation of market failures', The Internet, Policy and Politics Conference, Oxford Internet Institute, University of Oxford (2016)

application of digital intelligence largely for private ends, as opposed to such NPD regularly being made available for research at minimal costs points to a failure of the market for NPD to service these objectives. Vast amounts of NPD and economic value is governed privately and under profit oriented organisational frameworks. Stewardship of data has the potential to alter this dynamic by creating institutions which are designed to promote trusted exchange in NPD for a variety of use cases. The fostering of trusted, repeatable exchange is the first step in the creation of accessible and efficient markets for NPD.

The development of a stewardship solution that can be adopted at scale, in a repeatable form, can help engender a shift of organisational forms in the market. This means that any stewardship solution – if deployed for the governance of NPD generally – may have an influence on contracting norms and firm behaviour in the context of NPD, by creating incentives for value-maximizing conduct in the future.[90] For example, market imperfections – such as the transaction costs associated with making NPD widely available in a safe manner in terms of storing such data, monitoring access permissions and ensuring non-commercial use of data – may arguably be reduced in a scenario where a stewardship model can effectively perform these functions. Institutional innovations in the design of these stewardship models can ensure that contracting norms and behaviours are aligned to societally beneficial objectives. The German example of requiring bank representatives on supervisory boards of joint-stock companies, discussed earlier, is instructive in this regard. The creation of representative governance mechanisms within these institutions may result in redressal of certain market failures or negative externalities. It is within this frame that this position paper explores the institutional design of stewardship frameworks for NPD. The development of mechanisms which can address these market imperfections, therefore, appears central to the task of shaping the future of the digital economy to meet the public interest.

A competitive ecosystem of stewards can help reorient the digital economy. The creation of these stewards is useful for three functions: first, it creates a blueprint for a repeatable framework in the context of NPD that can be used to design institutions which are oriented to the public good; second, through mechanisms such as data sharing policies, or the procurement of NPD from private companies and public agencies, these stewards can ensure that data which is concentrated amongst a few entities can be made widely accessible and socially useful; and thirdly, in a scenario where multiple such stewards exist, it is likely to incentivise these stewards to act in a manner which secures their position in this ecosystem. This is likely to engender secure data sharing practices, promote benefit sharing agreements, create an accessible market and create an alternative for communities to trust with their data.

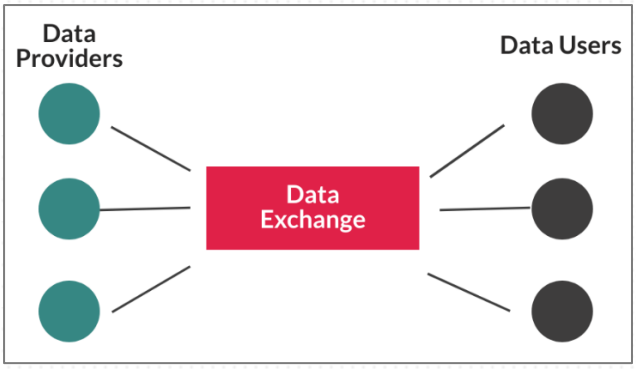
To this end, this chapter examines some of the broad archetypes of stewardship models that are commonly discussed in relation to NPD and 'data commons'. It goes on to identify a set of design principles for building a knowledge-commons, adapted from Elinor Ostrom's work, through which a comparative analysis of these models can be conducted. Finally, it compares the models of data stewardship along these design principles to identify which archetype of stewardship appears best placed to satisfy these principles.

[90] Posner, Richard. Economic Analysis of Law (1977).

# Types of stewardship models

Data stewardship arrangements can be oriented towards different goals. An examination of pilot projects around the world reveals that a series of different mechanisms are used to achieve these objectives. Some of the commonly seen stewardship models are discussed briefly herein:

## Data Exchanges

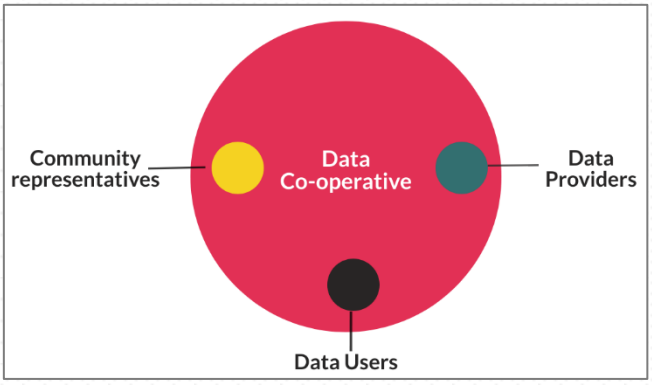



Data exchanges operate as centralised or decentralised platforms, whose primary function is to facilitate trade in data through their platform. The platform's role is ordinarily limited to providing common standards, putting in place security measures, providing common policies for use of the platform and setting entry restrictions.

A data exchange is primarily geared towards facilitating interactions between end-users and data sharers. A data exchange offers individual data sharers a high degree of control over how their data is shared and they directly engage with end-users through the platform of the data exchange. A data exchange, since it facilitates direct interactions between end-users and data sharers, places their interests at the fore of data sharing. Other stakeholders, however, have limited avenues for intervention in this exchange. For example, the role of the data exchange, being limited to setting common standards, offers limited controls to the community over data access and usage, which is largely governed by the negotiated terms between the data sharer and end-users.

Due to its limited role in the governance of these interactions, it may not be well-suited to impose an enforceable duty to protect the public interest. The role of the data exchange is ordinarily limited to enabling market transactions by providing common standards and setting entry restrictions. Data sharing is subject to the operation of market forces, where stakeholders and their representatives have limited means of intervention.

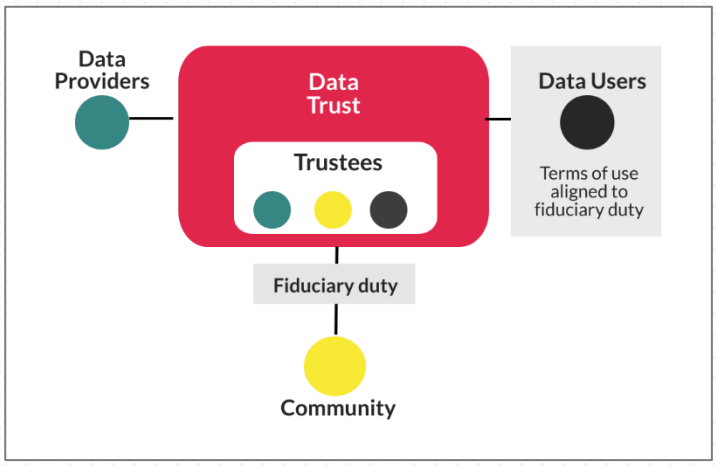
## Data Co-operatives




A data co-operative is a collective for the pooling and management of data and is governed by the rules that are developed by the collective. The members of the collective have multiple avenues to represent their interests and participate in the governance and operation of the data co-operative. However, stakeholders who are not a part of the collective are excluded from this process and lack effective means for their interests to be heard.

A data co-operative allows the members of the co-operative to pool their data and facilitates its sharing, and these members can collectively set and enforce rules regarding data access and use. Further, a data co-operative can be placed under a duty to act in the public interest. The members of the collective have a significant role in the formation, modification, and enforcement of these rules. Consequently, the efficacy of this model in actualising such a duty depends on the way in which its members choose to act and presents a variable risk of capture. Ordinarily, entities must be a part of this collective to engage in this exercise, which limits the degree to which it can enable large-scale data sharing or factor in the interests of other stakeholders.

# Data Trusts




A data trust draws on the idea of a legal trust, which is a centralised independent body holding an asset for the primary benefit of the beneficiary of the asset. In legal terms, this is referred to as the fiduciary duty of the asset-holder, who is termed the trustee. It is being increasingly advocated as a safe and trusted data stewardship model, especially in the context of smart cities.[91] A data trust can essentially be described as "a structure where data is placed under the control of a board of trustees with a fiduciary responsibility to look after the interests of the beneficiaries."[92]

A data trust can be a contract that gives an individual or a group of trustees, the authority to make decisions regarding the use of data on behalf of others.[93] It can also be defined as a data sharing arrangement between data subjects and data collectors, whereby a data subject is the settlor of the trust by giving away data as an asset, and assumes the role of a beneficiary.[94] This is similar to the concept of a 'bottom-up' trust, where the data subjects or providers are both the trust settlors or authors and its beneficiaries.[95] The steward or manager of a data trust is ideally expected to be an independent entity, which is not the data provider or data user/beneficiary. While providers and users/beneficiaries can have a say in the decision-making of the trust, they should not occupy an overly dominant or biased role.[96] In some conceptualisations, these entities can serve as vehicles for collective bargaining with companies, on behalf of a larger mass of users or the community. These conceptualisations, such as a 'bottom-up' data trust or personal data stores, may be suitable in the context of personal data. In the context of non-personal data, data trusts may take the form of 'civic data trusts', with obligations defined at a community-level instead of towards individuals.

While the existing models of data trusts that have been studied vary in their conceptual proximity to the actual legal structure of a legal trust, the core ideas that are common to these conceptions are – (a) the existence of a trustee, or someone bestowed with the responsibility of managing the data and ensuring its safety, (b) the use of that data in the best interests of the beneficiary, and (c) recognising the public as stakeholders within the stewardship framework.

[91] Teresa Scassa, 'Some thoughts on Smart Cities and Data Governance', 25 November, 2018 <www.teresascassa.ca/index.php?option=com_k2&view=item&id=293:some-thoughts-on-smart-cities-and-data-governance&Itemid=80> Accessed 14 April 2020; Natasha Tusikov, '"Urban Data" & "Civic Data Trusts" in the Smart City', CENTRE FOR FREE EXPRESSION BLOG, 06 August, 2019 <available at https://cfe.ryerson.ca/blog/2019/08/"urban-data"-"civic-data-trusts"-smart-city> Accessed 14 April 2020.

[92] Anouk Ruhaak, 'Data Trusts: Why, what and how', available at < https://medium.com/@anoukruhaak/data-trusts-why-what-and-how-a8b53b53d34> Accessed 10th October 2020

[93] Bianca Wylie and Sean McDonald, 'What Is a Data Trust?', 09 October 2018 <https://www.cigionline.org/articles/what-data-trust> Accessed 14 April 2020.

[94] Lilian Edwards, 'The Problem with Privacy' (2004) 18(3) International Review of Law Computers & Technology 263.

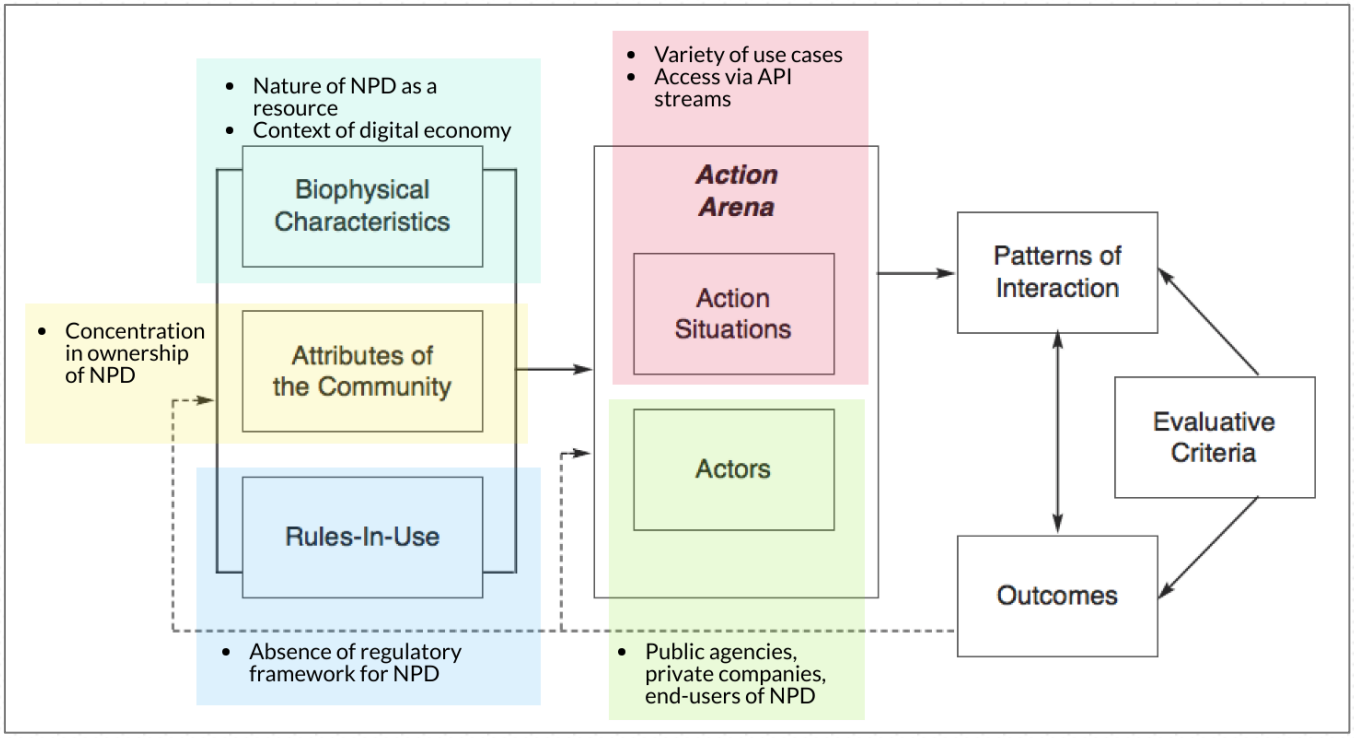
[95] Sylvie Delacroix and Neil D Lawrence, 'Bottom-up data Trusts: disturbing the 'one size fits all' approach to data governance', (2019) 9(4) International Data Privacy Law 236.

[96] Open Data Institute, ''Data trusts: lessons from three pilots' (2019), <https://docs.google.com/document/d/118RqyUAWP3WIyyCO4iLUT3oOobnYJGibEhspr2v87jg/edit> accessed 14 April 2020.

# Principles for designing a commons-oriented stewardship model

There are some broad models of data stewardship that are discussed above, but there is no definitive conceptualisation of what these models practically amount to. There are several pilots which claim to fit any of the labels described above, but in actuality have significant variance in terms of their governance structure, operational practices and other specifics. Consequently, there is no clear blueprint for what amounts to a 'data exchange, a 'data co-operative' or a 'data trust'. Several of the projects which describe themselves as a "data trust" operate in many different forms – sometimes as a community-led cooperative, such as Midata.Coop, or at other times, a profit-making company, such as Sightline data trusts. The broad labels allocated to each stewardship model may be unhelpful in identifying what it would mean for a "data trust" to be adopted, as opposed to a "data co-operative". Therefore, it is important to begin from first principles and identify the design principles that would be a part of an optimal stewardship model. Based on these principles, we compare the models listed above to identify which descriptor best aligns with the principles of an optimal stewardship model.

Based on her study of governance frameworks for commons, Ostrom proposed eight design principles that are likely to enable the effective management of natural resources.[97] These are based on the application of the Institutional Analysis and Development (IAD) Framework, which evaluates the characteristics of the resources involved, the attributes and roles of community members, and the "rules-in-use" of the commons framework to evaluate its efficacy.[98] The IAD framework and the principles identified served as the starting point of evaluating principles that can similarly apply to a data commons.[99]




[97] Janis Wong and Tristan Henderson, 'Co-Creating Autonomy: Group Data Protection and Individual Self-determination within a Data Commons', (2020) 15(1) International Journal of Digital Curation, 16. (The eight principles include clearly defined boundaries and clear identification of the participants, congruence between appropriation and provision rules and local conditions, collective-choice arrangements, monitoring, graduated sanctions, conflict resolution, recognition of the rights to organise, and nested enterprises.)

[98] Elinor Ostrom and Charlotte Hess, 'A Framework for Analyzing the Knowledge Commons' in Elinor Ostrom and Charlotte Hess (ed), *Understanding Knowledge as a Commons: From Theory to Practice* (2007) 41, 42.

[99] Parminder Jeet Singh, 'Data and Digital Intelligence Commons (Making a Case for their Community Ownership)', available at <https://itforchange.net/sites/default/files/1673/Data-commons.pdf> Accessed 24 June 2020

## Adapting the Ostrom Principles for a Knowledge Commons

The principles developed by Elinor Ostrom need to be adapted for establishing an urban data commons based on an analysis of the scholarship on the robustness of these design principles, their adaptation to the 'knowledge commons', and the application of the IAD framework in urban contexts. This is due to a few key distinguishing features of data, when compared with natural resources as outlined below:

- **Nature of the resource:**
  The resource, i.e. data may imply a broad, global set where the resource is expected to keep growing through its use and subsequent knowledge creation. Furthermore, data or information as a commons resource has different considerations regarding use - unlike a natural resource, it isn't liable to overuse. On the other hand, its value and resourcefulness grow with greater use, which incidentally adds back to the resource.

- **Global and amorphous communities:**
  Housed on facilities like the internet, a data commons is likely to be global in nature, where communities represent a multiplicity of interests. For instance, data providers may wish to tap into other datasets, users wish to develop research or develop commercial applications, while the public may wish to have access to low cost mobility solutions based on the use of this data. This is contrasted against more homogenous localised communities in the case of natural resource commons.

- **Complexity of relationships:**
  Scholars studying urban commons have also highlighted the complexity of relationships within the city, noting that urban resources are often governed through several layers of existing regulatory and political actors. Their relationships are inextricably linked with the rules governing data and knowledge, which need recognition as core components of the commons. Further, any commons-based solutions will require simultaneous change in existing laws and administrative structures.

- **Layered governance:**
  Further, the diversity of community members with heterogeneous interests requires layered governance mechanisms. Therefore, it is necessary to account for the role played by state actors and private entities, which can nevertheless help in providing better access to resources.

- **Fiduciary duties:**
  In knowledge and natural resource commons, trust is established based on interpersonal relationships within the community. On the other hand, in a data commons framework, where interpersonal relationships are hard to find, and where a multiplicity of interests are involved, recognising the fiduciary responsibilities of the steward is one mechanism of addressing trust and legitimacy related challenges.

# Design principles for data stewardship models

The discussion on different types of 'stewardship' models points to the importance of the enforceability of the duty to act in favour of another. If an institutional structure for designing data commons is to be identified, then the ability of this structure to act as a 'steward' of data assumes importance. The legal instrument which enforces this concept of stewardship can be contractual, trust-based or statutory. This basic duty, regardless of the specific form it takes, for the purpose of this paper, is referred to as an "enforceable fiduciary responsibility". The centrality of this duty to the stewardship model being set out here can be considered an additional design principle – drawing explicitly from the challenges faced in establishing trust-based relationships and solving legitimacy issues in designing knowledge commons.

Keeping these nuances in mind, emerging from existing scholarship on knowledge 'commons', we narrow down on the following design principles for designing a data commons:

## 1. An enforceable fiduciary responsibility

A fiduciary duty, to act in utmost good faith for the benefit of the community can help engender trust and address challenges associated with competing interests within a complex and heterogeneous data commons.[100] In the data commons, formal governance structures wherein the fiduciary role is recognised can then undertake complex determinations in ensuring that the data is managed according to the purposes[101] of the commons, say protecting the privacy and security of communities, while generating value through use of the data. The form of this duty can differ according to particular legal systems.


## 2. Multi-stakeholder governance schemes

In the context of a data commons, the resource would be best defined as the repository of pooled information.[102] Similarly, the community of actors using the resource would be defined by all those pooling the information, using it, and benefiting from its use.[103] Since the laws governing the information and the community members' *inter-se* relationships are inextricable from rules of use, collective governance engaging multi-stakeholder schemes and partnerships are necessary for designing a data commons.[104]

[100] While a localised commons is likely to find trustworthy management owing to the presence of strong interpersonal relationships within a small community, this can be difficult to expect in a dispersed data commons involving corporate entities.

[101] Paul B. Miller and Andrew S. Gold, 'Fiduciary Governance', (2015) 57 William and Mary Law Review 513.

[102] Mayo Fuster Morell, 'Governance of Online Creation Communities for the Building of Digital Commons: Viewed through the Framework of Institutional Analysis and Development' in Brett Frischmann, Michael Madison et al (eds.), *Governing Knowledge Commons* (Oxford University Press, 2014) 281.

[103] Brett Frischmann, Michael Madison et al, 'The Knowledge Commons Framework' in Brett Frischmann, Michael Madison et al (Eds.), *Governing Medical Knowledge Commons* (Cambridge University Press, 2017) 9 ("*Knowledge commons members often come together for the very purpose of creating particular kinds of knowledge resources. The relevant community thus is determined not by geographical proximity to an existing resource, but by some connection – perhaps of interest or of expertise – to the knowledge resources to be created*").

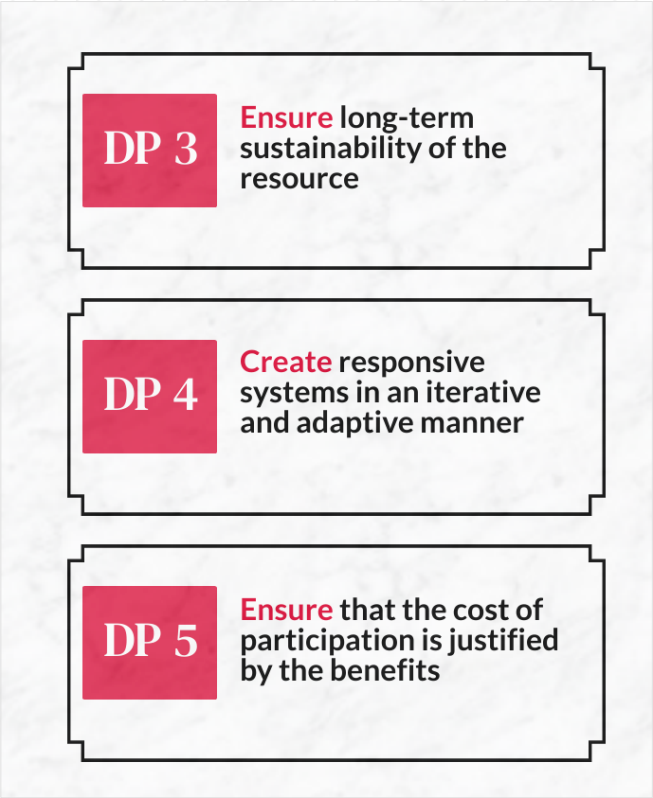
[104] Sheila Foster and Christian Iaione, 'Ostrom in the City: Design Principles for the Urban Commons' (2017), available at < https://www.thenatureofcities.com/2017/08/20/ostrom-city-design-principles-urban-commons/> Accessed June 26, 2020.

## 3. Sustainability of the repository

The data commons should be able to sustain itself in the face of relatively rapidly changing participants, technology and concomitant laws.[105] It is further important to ensure sustainability of the commons wherein participants (i.e. data providers and data users) remain committed to sharing their data despite changes in leadership.[106]

## 4. Iterative and adaptive systems

Frameworks that are adaptive to technological changes[107], and open to rectification (especially where heterogeneous communities require iterative approaches)[108] are necessary for the sustenance of the data commons.[109] Some elements of a robust and adaptive governance framework include information sharing, conflict resolution, ensuring compliance with rules, providing the requisite infrastructure and being prepared for change.[110]




## 5. Efficient participation

The commons framework should ensure economic efficiencies where the cost of participation is justified by the benefits derived.[111] Economic efficiency has two specific considerations attached:

a. **Equity:** It is important to factor in potential redistribution and competition concerns that arise with collective pooling of the data.[112]
b. **Informed Choices:** The participants should have the relevant information to help them decide if participation makes sense for them.[113] This includes mechanisms to measure and monitor the outcomes of pooling and participation. For example, Transport for London's data sharing platform provided information on the relative benefits of open data sharing in the form of cost savings to demonstrate its effectiveness.

[105] Elinor Ostrom and Charlotte Hess, 'A Framework for Analyzing the Knowledge Commons' in Elinor Ostrom and Charlotte Hess (ed), *Understanding Knowledge as a Commons: From Theory to Practice* (2007) 41, 63-64.

[106] Elinor Ostrom and Charlotte Hess, 'A Framework for Analyzing the Knowledge Commons' in Elinor Ostrom and Charlotte Hess (ed), *Understanding Knowledge as a Commons: From Theory to Practice* (2007) 41, 63-64.

[107] Sheila Foster and Christian Iaione, 'Ostrom in the City: Design Principles for the Urban Commons' (2017), available at < https://www.thenatureofcities.com/2017/08/20/ostrom-city-design-principles-urban-commons/> Accessed June 26, 2020.

[108] Elinor Ostrom and Charlotte Hess, 'A Framework for Analyzing the Knowledge Commons' in Elinor Ostrom and Charlotte Hess (ed), *Understanding Knowledge as a Commons: From Theory to Practice* (2007) 41, 68.

[109] Elinor Ostrom and Charlotte Hess, 'A Framework for Analyzing the Knowledge Commons' in Elinor Ostrom and Charlotte Hess (ed), *Understanding Knowledge as a Commons: From Theory to Practice* (2007) 41, 68.

[110] Elinor Ostrom and Charlotte Hess, 'A Framework for Analyzing the Knowledge Commons' in Elinor Ostrom and Charlotte Hess (ed), *Understanding Knowledge as a Commons: From Theory to Practice* (2007) 41, 66.

[111] Michael Cox, Gwen Arnold et al, 'A Review of Design Principles for Community-based Natural Resource Management', (2010) 15(4), Ecology and Society 38.

[112] Elinor Ostrom and Charlotte Hess, 'A Framework for Analyzing the Knowledge Commons' in Elinor Ostrom and Charlotte Hess (ed), *Understanding Knowledge as a Commons: From Theory to Practice* (2007) 41, 65.

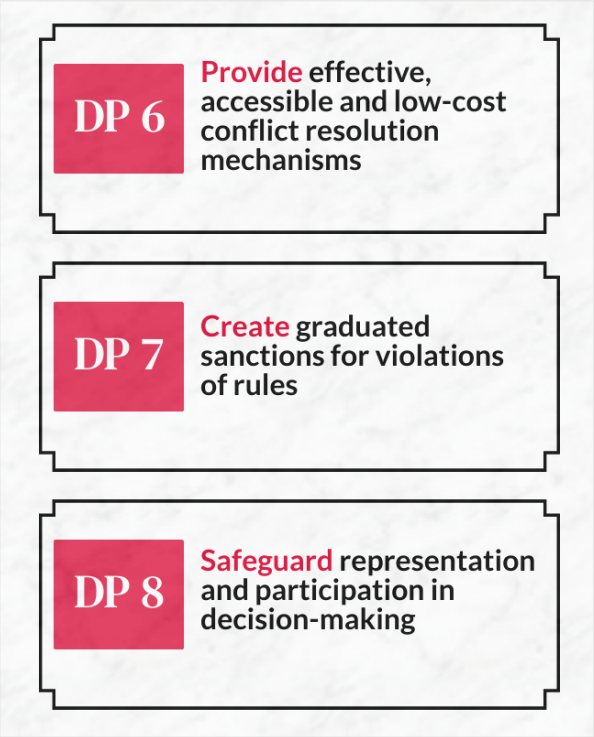
[113] Elinor Ostrom and Charlotte Hess, 'A Framework for Analyzing the Knowledge Commons' in Elinor Ostrom and Charlotte Hess (ed), *Understanding Knowledge as a Commons: From Theory to Practice* (2007) 41, 67.

## 6. Effective and low-cost conflict resolution:

Conflict resolution that is effective and accessible to participants is necessary to maintain cohesion within the commons where diverse interests are expected to subsist. This entails developing mechanisms that allow space for everyone to be heard and grievance redressal to take place in a manner which is "*legitimate, fair, and scientifically sound.*"[114]

## 7. Graduated sanctions for rule compliance:

For effective enforcement of rules, sanctions should be developed such that they are proportionate to the violation, and the custodian is seen as legitimate and effective to ensure trust in the system.[115] These formal sanctions complement incentives, commitments, and subtle social sanctions within the overall governance framework.[116]




## 8. Participation in designing collective action agreements:

Collective action problems, i.e. problems relating to the welfare of the commons, should be addressed through participatory mechanisms which allow all members of the community to voice their concerns and make decisions. Participation is also necessary at the level of modifying operational rules.[117] Inclusivity and representation in a complex and layered commons is likely to require civil society actors, expert-developed standards, and engagement of local governments to drive participation.[118]

Participation is necessary across each level of decision-making:

1. At the **constitutional level,** to define who participates in the commons and its governance. This may take the form of charter documents of the commons.[119]
2. At the **collective choice level,** at the policy level of rules to define the responsibilities vis-à-vis the administration of the commons. This may include the rules for accessing and using the data, sanctions for non-compliance, etc.
3. At the **operational level,** to define the rules pertaining to who may submit, what they may submit, and how they may do so. In the data commons context, this may take the form of data upload policies.

[114] Elinor Ostrom and Charlotte Hess, 'A Framework for Analyzing the Knowledge Commons' in Elinor Ostrom and Charlotte Hess (ed), *Understanding Knowledge as a Commons: From Theory to Practice* (2007) 41, 67.

[115] Michael Cox, Gwen Arnold et al, 'A Review of Design Principles for Community-based Natural Resource Management', (2010) 15(4), Ecology and Society 38.

[116] Elinor Ostrom and Charlotte Hess, 'A Framework for Analyzing the Knowledge Commons' in Elinor Ostrom and Charlotte Hess (ed), *Understanding Knowledge as a Commons: From Theory to Practice* (2007) 41, 67.

[117] Michael Cox, Gwen Arnold et al, 'A Review of Design Principles for Community-based Natural Resource Management', (2010) 15(4), Ecology and Society 38.

[118] Natalie Chyi and Yuliya Panfil, 'A Commons Approach to Smart City Data Governance: How Elinor Ostrom Can Make Cities Smarter' (2020), available at <https://www.newamerica.org/future-property-rights/reports/can-elinor-ostrom-make-cities-smarter/principle-4-promote-responsibility-for-data-governance-among-multiple-layers-of-nested-enterprises> Accessed 24 June 2020.

[119] Elinor Ostrom and Charlotte Hess, 'A Framework for Analyzing the Knowledge Commons' in Elinor Ostrom and Charlotte Hess (ed), *Understanding Knowledge as a Commons: From Theory to Practice* (2007) 41, 50.

## 9. Monitoring compliance:

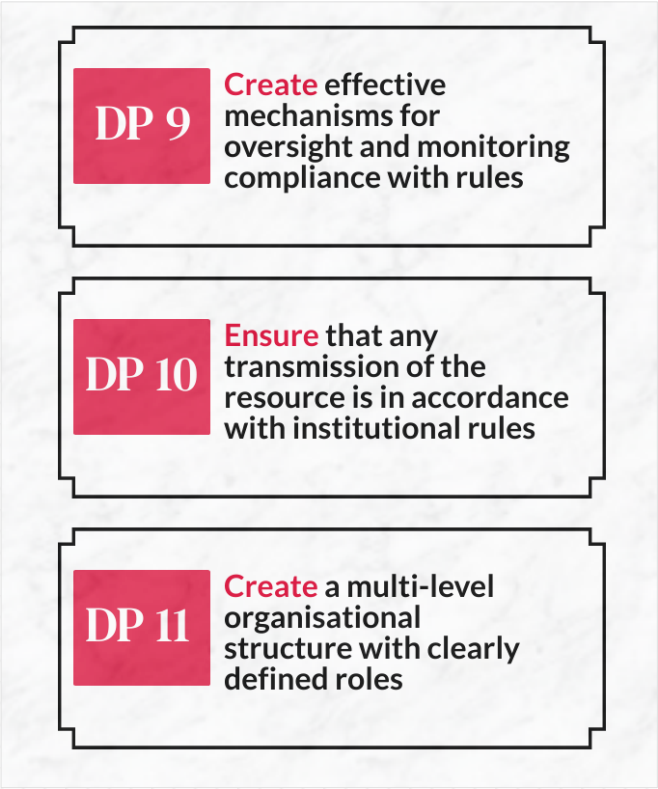
Ensuring compliance with the rules of the commons should comprise a combination of controls built into the technical infrastructure such as audit mechanisms, tracking use, etc, and a trustworthy monitor whose interests are aligned with the community's.[120] Effective monitoring also comprises oversight mechanisms to oversee the monitor.[121]

## 10. Regulation of transmission through rules in use:

Transmission rules that are actionable need to be developed to ensure the privacy and safety interests of the community, while ensuring that data continues to be shared under the commons.[122]

## 11. Nested enterprises:

The organisation structure of the data commons should comprise a set of interconnected levels of operations, or a 'nested' structure with clearly defined roles for each level.[123] In the case of municipal or city resources, this may involve a clear definition of rules for their management by different levels of the government (local, state, national) as well as individuals.[124]




[120] Michael Cox, Gwen Arnold et al, 'A Review of Design Principles for Community-based Natural Resource Management', (2010) 15(4), Ecology and Society 38 ("*in order to ensure that the monitor does not go rogue and performs its duties effectively, there is a need to evaluate incentives, and linking the well-being of the resource management with their own interests. This could involve picking someone from the community itself, whose self-interests are tied to the welfare of the community or involve monitoring mechanisms that integrate oversight over them*").

[121] Michael Cox, Gwen Arnold et al, 'A Review of Design Principles for Community-based Natural Resource Management', (2010) 15(4), Ecology and Society 38

[122] Madelyn Sanfilippo, Brett Frischmann and Katherine Standburg, 'Privacy as Commons: Case Evaluation Through the Governing Knowledge Commons Framework.' (2018) 8, Journal of Information Policy 116 (Unlike a knowledge commons, which typically espouse open sharing, a data commons may need to restrict data sharing to prioritise the privacy interests of the community members. In such a case, the obvious choice may not necessarily mean secrecy or cordoning off access to the data, but to maintain an "*appropriate flow of personal information*").

[123] Natalie Chyi and Yuliya Panfil, 'A Commons Approach to Smart City Data Governance: How Elinor Ostrom Can Make Cities Smarter' (2020), available at <https://www.newamerica.org/future-property-rights/reports/can-elinor-ostrom-make-cities-smarter/principle-4-promote-responsibility-for-data-governance-among-multiple-layers-of-nested-enterprises> Accessed 24 June 2020.

[124] Natalie Chyi and Yuliya Panfil, 'A Commons Approach to Smart City Data Governance: How Elinor Ostrom Can Make Cities Smarter' (2020), available at <https://www.newamerica.org/future-property-rights/reports/can-elinor-ostrom-make-cities-smarter/principle-4-promote-responsibility-for-data-governance-among-multiple-layers-of-nested-enterprises> Accessed 24 June 2020.

# Assessing models of data stewardship

Based on the above design principles, we examine some common models of data stewardship to analyse which model would be best suited to materialise these principles. It should be noted that, as previously discussed, the labels used to describe a particular model of data stewardship are fairly indeterminate. Therefore, the phrase "data co-operative" may refer to a wide variety of different organisational forms. Therefore, this analysis proceeds on the basis of the conceptualisation of each model as set out in the initial portions of this chapter. It is possible that an organisation which uses any of the following descriptors may satisfy the design principles listed below, while in our analysis, it is indicated as otherwise.

**Key:**

| | |
|---|---|
| | Does not appear to satisfy |
| | May partially satisfy |
| | May satisfy |

| Design Principle | Data Exchange | Data Co-operative | Data Trust | Summary |
|---|---|---|---|---|
| An enforceable fiduciary duty | | | | A fiduciary duty can be enforced on the trustees of a data trust via a charter document. While a fiduciary duty can be a part of the charter documents of a co-operative, its members ultimately determine the efficacy of such a duty. The limited role of a data exchange appears to not provide sufficient avenues for the imposition of a fiduciary duty. |
| Presence of multi-stakeholder governance schemes | | | | While multi-stakeholder governance schemes are possible in all models, these schemes would have to be designed in any stewardship model, given the lack of an existing blueprint for such schemes. In data co-operatives, specifically, stakeholders who are not a part of the co-operative may be excluded in any governance scheme of the co-operative. In a data trust and data exchange, the charter documents can require such governance schemes, though in a data exchange, the platform ordinarily decides on its own business affairs, and is not necessarily required to conduct multi-stakeholder governance. |
| Sustainability of the repository | | | | The sustainability of the repository in a data exchange depends on the willingness of individual data providers to keep coming back to the exchange. Data providers would be a part of the co-operative, and therefore, bound to provide their data to the co-operative as long as they continue being members. In a data trust, while data providers can be made a part of the trust's structure, and therefore, create a degree of commitment – it is possible for data providers to opt-out of the structure. |
| Iterative and adaptive systems | | | | It is possible for systems across all models to be iterative and adaptive, therefore this evaluation is done based on the variety of stakeholders whose feedback would necessarily have to be considered in any such iteration. While most data trusts and co-operatives appeared to adopt some form of periodic collective review, data exchanges are largely seen to operate as mere platforms, without participatory governance initiatives. |

| | | | | |
|---|---|---|---|---|
| Efficient participation | | | | The costs of participation in an exchange and a trust remain low for data providers as well as other users. Co-operatives may require membership or financial commitments from their users, which may increase the costs of participation. |
| Effective and low-cost conflict resolution | | | | A data exchange, given its limited role in the transaction, may be at a relative disadvantage in providing effective conflict resolution. Co-operatives and trusts can provide these mechanisms as part of their charter documents which govern all data sharing under these mechanisms. |
| Graduated sanctions for rule compliance | | | | The contractual terms of data sharing can have graduated sanctions across all three models. |
| Participation in designing collective action agreements | | | . | A data exchange, which merely provides a platform for data sharing, does not necessarily require participation in designing collective action agreements. While a co-operative requires this participation, it is ordinarily only extended to members of the co-operative. A data trust, such as the potential civic data trusts, on the other hand, can require broader degrees of participation which is hard wired into its charter documents, with no limitation on such participation being restricted to its members. |
| Monitoring compliance | | | | Monitoring the compliance of a data exchange depends on the degree of transparency adopted by the provider of the exchange. A data co-operative has relatively more mechanisms for monitoring compliance, however their efficacy depends on the willingness of its members to undertake such monitoring and the degree to which they decide to provide it in their charter documents. A data trust, by virtue of its fiduciary duty, as well as the hard-wired obligations in its charter, can be made subject to monitoring and transparency requirements. |
| Regulation of transmission through rules in use | | | | All models of data stewardship can create rules – through contracts, licenses or other mechanisms – which regulate how the data is to be shared. The role of a data exchange, however, is usually limited to setting common policies and specifying formats, and therefore, may be relatively minor in comparison to the other models of stewardship. |
| Nested enterprises | | | | A data exchange is a platform and ordinarily, does not have the scope for multi-layered governance in nested, hierarchical forms. While such enterprise may be possible in a co-operative, it would be limited to its members. A data trust, on the other hand, by virtue of its charter documents, can be designed to have nested, hierarchical governance mechanisms which are not limited to its members. |

Based on this evaluation, the insufficiency of conventional arrangements in satisfying optimal design features of stewardship models becomes visible. For the purposes of this paper, it appears that a data trust would be effectively placed to be designed in a manner that satisfies the design principles outlined in this section. The **flexibility** offered by the relatively nascent concept of "data trusts", the **legal concept of a trust** and associated fiduciary duties, **the existence of a charter document** that can specify the precise manner in which a data trust will function, and the ability of its governance structure **to include stakeholders beyond its members or data providers** are the key factors which enable the design of the data trust in this manner. While the ideas of data exchange and data co-operative are also indeterminate and could be designed to satisfy these design principles and provide effective solutions as well, the limitations of the other models, based on a common understanding of such models, indicates that data trusts are an effective descriptor for the stewardship solution discussed in this position paper.

# Chapter III:

# Operationalising a data trust

The previous chapters explored the desirability of a stewardship model for enabling sharing of NPD and examined the contours of what an optimal stewardship model would look like. In this chapter of the position paper, the focus will be on how such stewardship models can be operationalised within the current legal framework.

To this end, this chapter will first identify a strategy for operationalising a data trust. It will look at available options for establishing non-profit organisations and constraints which are present in this process. These constraints indicate the necessity for certain legislative and policy changes that can be effectuated to make data trusts a reality.

Based on this analysis, this chapter examines how a prototype may be operationalised within the existing legal framework for it to resemble a data trust as far as possible, in terms of fiduciary responsibilities and a public-centric data stewardship model. Therefore, what is proposed within this chapter may not necessarily be classified as a data trust, but more of a legal entity with its trappings. It will look at the proposed governance and operational mechanisms of such a trusted intermediary and set out a proposed blueprint for operationalising such a model.

Our analysis will first identify various options that are available to legally structure such an entity. Secondly, we evaluate the constraints that exist within these current legal frameworks. Finally, we evaluate the viability of these structures to effectively serve as a quasi-data trust.

## Identifying options

Based on the discussion in the previous chapters, the concept of a data trust would take the form of an institution which enables participatory governance in the sharing of data for a public benefit.[125] This implies that a data trust should not be oriented around the concept of generating private gain or profiteering from the data that is shared by it. Therefore, an inquiry into the way an entity like this can be structured may be limited to other kinds of non-profit entities.

Further, based on a review of practices in other jurisdictions where entities which claimed to be data trusts were established, the most common forms appear to be cooperative societies and non-profit companies. The analogous legal structures to these in the Indian context, respectively, are registered societies, Section 8 companies and public charitable trusts. Legal trusts are considered since they are the legal structures that data trust are based on.

**Registered Societies** are constituted under the Societies Registration Act, 1860.[126] Seven or more persons can come together under this Act to register a society for the purposes outlined in Section 20 of the Act, which includes "*societies established for the promotion of science, literature, or the fine arts for instruction, and the diffusion of useful knowledge*".[127] This society is governed by its own rules and regulations, commonly referred to as the by-laws of a society.

**Section 8 companies** can be incorporated under the Companies Act, 2013 for the 'charitable objects' of "*the promotion of commerce, art, science, sports, education, research, social welfare, religion, charity, protection of environment or any such other*

[125] Sylvie Delacroix and Neil D Lawrence, 'Bottom-up data Trusts: disturbing the 'one size fits all' approach to data governance', (2019) 9(4) International Data Privacy Law 236.

[126] Societies Registration Act, 1860

[127] Societies Registration Act, 1860, s 20

*object*."[128] As per the Companies Act, 2013, these companies are prohibited from distributing their profits as dividend to its shareholders. This ensures that while the company can make profits, these profits have to be applied towards promoting its 'charitable objects'. Finally, section 8 companies are provided various exemptions from provisions of the Companies Act, 2013, which reduce their compliance cost vis-à-vis a for-profit company.[129]

**Public charitable trusts** are created by a trust deed, where some property is settled with the trust to govern this property in accordance with the terms of the trust deed in the interests of the public.[130] They can be registered under various State Acts related to such trusts, such as the Bombay Public Charitable Trusts Act, 1950, and are governed by the general principles of trust law. There is no central legislation which governs public charitable trusts, and the Indian Trusts Act, 1882 is limited to private trusts.

Globally, the use of legal trusts for a data trust has remained theoretical. [131] This is largely due to the rigidity of trust laws and the relative flexibility provided by other non-profit structures, a question which is explored in further detail in the next section.

# Recognising constraints

## 1. Characterisation of data as 'property' for trust law

The obvious implication from the phrase 'data trust' is the idea of a legal trust. This implication is present in various academic texts on the question of data trusts as well. However, a divergence is noticed when looking at examples of projects which have described themselves as 'data trusts'. While academic literature often extols the use of legal trusts for the establishment of a data trust, most of the data trusts which have actually been implemented do not actually take the form of a legal trust. This divergence points to an important question regarding the use of the nomenclature of 'data trusts' – whether the legal framework of trusts is fit-for-purpose for establishment of 'data trusts'? To explore this question, we look at two important inquiries that may help answer it: *first*, whether trust law, theoretically, is fit-for-purpose for establishing data-based trusts, and *secondly*, whether trust law in India, from a practical perspective, enables the establishment of data-based trusts.

### a. Theoretical problems with framing NPD as property

The primary question which seems to prevent the applicability of trust law to data-based trusts is the rigid requirement in trust law related to the concept of 'property'. Put briefly, trust law has evolved to provide for governance of property in the interests of some beneficiaries. The prerequisite for any resource to be the subject matter of a trust,

[128] Companies Act, 2013, s 8

[129] ICSI FAQ on the Companies Act, 2013, available at <https://www.icsi.edu/media/portals/0/FAQs_on_the_Companies_Act_2013_revised_28-04-14.pdf> Accessed 18 May 2020.

[130] Graham Moffat, Trusts Law (4th Ed, 2005) at 515.

[131] For instance, the Open Corporates Data Trust, which pools corporate data to be applied for public benefit, does not use a legal trust. Instead, it uses a corporate structure entailing a corporate entity set up to perform the functions of a trust, i.e. ensuring that the operational entities operate as per the rules and policies set out by it. See Anonymous, 'A corporate structure for the public good, Part 2: basic structure', OpenCorporates Blog (2017) <https://blog.opencorporates.com/2017/10/25/a-corporate-structure-for-the-public-good-part-2-basic-structure/> accessed 04 April 2020; Sidewalks Labs had decided against structuring their data trust as a legal trust, because they did not find legal trusts suitable for benefitting the general public interest, and instead opted to set it up as a not-for profit entity set up by the public authorities, *see* 'Digital Innovation' <https://storage.googleapis.com/sidewalk-toronto-ca/wp-content/uploads/2019/06/23143337/MIDP_Vol.2_Chap.5_DigitalInnovation.pdf> Accessed 14 April 2020; The National Health Information Exchange (NHIN) inbuilds the trust requirement through a Data Use and Reciprocal Support Agreement (DURSA), which is a multiparty legal agreement. See Nationwide Health Information Network, 'Nationwide Health Information Network (NHIN) Exchange: Architecture Overview' (2010), available at <https://www.healthit.gov/sites/default/files/nhin-architecture-overview-draft-20100421-1.pdf> Accessed 14 April 2020.

therefore, is that the resource must be able to be classified as 'property'.[132]

This leads to the question of whether non-personal data can appropriately be treated as 'property' or not, under Indian law. At its core, this question is more normative than descriptive[133] – and in order to resolve this, the question must first be asked – what is property and whether non-personal data can appropriately be considered within the definition of property?

Property has generally been defined as "*the right to possess, use, and enjoy a determinate thing*", or "*any external thing over which the right of possession, use and enjoyment are exercised*".[134] In Indian jurisprudence, the term property, in the context of intangible assets, has been described as "*that dominion or indefinite right of use or disposition which one may lawfully exercise over particular things or subjects*".[135] These understandings broadly lead to the notion of looking at property as a "bundle of rights" that may be exercised by a person in respect of a particular thing.[136]

One of the issues relevant to this discussion is whether there is a bundle of rights that can appropriately be identified in respect of non-personal data. If a person can be identified as having this "dominion" or "indefinite right of use" – then it may be forthcoming to treat non-personal data as property.[137] This dominion does not need to be absolute in nature, but a substantial number of the rights implicated in this "bundle of rights" should ideally be identifiable and attributable to a definite entity in order for some sort of ownership to be attributed. However, where such categorisation is not possible, the concept of data as property may no longer be a persuasive characterisation for the reasons outlined earlier.

Notably, and especially in the context of non-personal data, it must be considered that this data is often produced jointly – through the efforts of both the persons who collect such data, and the persons who produce such data.[138] For example, in the context of urban mobility data (UMD), while transit agencies may install sensors and collect information about people's transport, it is the people who participate in these systems and therefore enable the generation and collection of this data. The intricate connection between people's bodies, their activities and the creation of data as a resource, and the joint efforts in producing this data, therefore, make the characterisation of non-personal data as 'property' to be owned by a singular person, challenging and legally questionable.[139] There is an emerging recognition of the shortcomings of treating 'data' as property[140] – both from the perspective of legal theory related to the concept of 'property' as well as economic perspectives on the digital economy.[141] These ideas should be duly considered before a characterisation of data as 'property' is forwarded. Particularly since being unable to characterise data as property may present an obstacle in operationalising a data trust through the legal structure of a trust. More importantly, a characterisation of this nature is an exercise for the legislature to enact, or for the judiciary to interpret.

The framing of 'community data', which was formulated in the Srikrishna Committee Report, has provided a lens through which non-personal data is conceptualised beyond its traditional notions as 'property'. This was taken further in the Report of the Committee of Experts on Non-Personal Data, which

[132] James E Penner, 'The (True) Nature of a Beneficiary's Equitable Proprietary Interest under a Trust', 27 Canadian Journal of Law and Jurisprudence, 473 (2014)

[133] Lalit Panda, 'The hybridisation of property, liability and inalienability in data protection', 3(2) Journal of Intellectual Property Studies, 18 (2020)

[134] *Property,* Blacks Law Dictionary, 1335-36 (9th ed., 2009).

[135] Vikas Sales Corporation v. Commissioner of Commercial Taxes, 1996 4 SCC 433.

[136] Vikas Sales Corporation v. Commissioner of Commercial Taxes, 1996 4 SCC 433.

[137] Jerry Kang, 'Information Privacy in Cyberspace Transactions', 50 Stanford Law Review, 1193, 1218 (1998)

[138] Jerry Kang, 'Information Privacy in Cyberspace Transactions', 50 Stanford Law Review, 1193, 1218 (1998)

[139] Anja Kovacs and Nayantara Ranganathan, 'Data sovereignty, of whom? Limits and suitability of sovereignty frameworks for data in India', Data Governance Network Working Paper 03 (2019)

[140] Anja Kovacs and Nayantara Ranganathan, 'Data sovereignty, of whom? Limits and suitability of sovereignty frameworks for data in India', Data Governance Network Working Paper 03 (2019)

[141] Anja Kovacs and Nayantara Ranganathan, 'Data sovereignty, of whom? Limits and suitability of sovereignty frameworks for data in India', Data Governance Network Working Paper 03 (2019)

marks a divergence from the traditional framing of data[142] as 'property' that would be owned by a particular individual or entity, say, a public transit agency. Given the rights of the broader community in this data, the manner of exercise of these rights must also be participatory and collective.[143] For example, a public agency, merely by virtue of being the collector of this data, should not be granted the exclusive privilege of determining the use of this data. However, if data is considered property for the subject matter of a trust, within existing frameworks of trust law, the data would have to be settled with the trust by those public agencies, who would legally be entitled to determine the terms of the trust deed.[144] This may undermine the concept of 'community data' as such, given the primary role given to the settlor in shaping the terms of the trust deed under current trust law.

### b. Practical issues with characterising NPD within trust laws

Commentators who have studied the various ways in which rights over data can be exercised largely point to three frameworks other than property – intellectual property[145] (which is defined and protected by statutory frameworks), privacy rights (which are exercised as a constitutional right), and confidentiality rights[146] (which can be exercised as a contractual right or a claim in tort law or equity).

First, in respect of intellectual property rights, in Indian law, NPD can be protected as intellectual property when it is compiled as a database and involves a minimum degree of skill or creativity in its compilation.[147] As such, not all raw non-personal data may qualify as intellectual property. For example, there may be no intellectual property over NPD such as transit routes and schedules, since they may not satisfy the test laid down in *EBC v. DB Modak*.[148] Furthermore, Indian case law on databases is fairly limited and does not adequately provide clarity regarding the legal status of databases such as the aggregated data sets of NPD used in modern analytics. However, if a database is indeed subject to copyright, it may arguably be considered intellectual property for the purposes of trust law.

Second, privacy in relation to personal data is not granted under a property-rights regime, but instead as a constitutional right.[149] In relation to non-personal data, there has been some recognition of the concept of 'group privacy' in the Report of the Committee of Experts on Non-Personal data – however, this emergent concept also appears rooted in constitutional concerns related to privacy, as opposed to a property-rights regime[150] - thereby being an unsuitable conceptual basis for framing NPD in trust law.

Third, in terms of property rights, the right to protect information from unauthorised access or disclosure is understood in common law as a contractually designated obligation of confidentiality.[151] The payment of consideration for information in common law, for example, has been understood not as indicating a transfer of property in the information, but as consideration for a promise to not disclose the information.[152] The right in relation to information, therefore, may be interpreted as a right to enforce the contract-based obligation of confidentiality which can be exercised by a person privy to the contract.[153]

---

[142] Report of the Committee of Experts on Non-Personal Data, Ministry of Electronics and Information Technology.

[143] Anouk Ruhaak, 'Data commons & Data Trusts', available at <https://medium.com/@anoukruhaak/data-commons-data-trust-63ac64c1c0c2> Accessed 25th August 2020

[144] *See* The Bombay Public Trusts Act, 1950.

[145] Eastern Book Company v. D.B. Modak, 2002 PTC 641

[146] Prashant Reddy, 'The Other IP Right: Is it time to codify the Indian law on protection of confidential information?', Journal of National Law University, Delhi (2018)

[147] Eastern Book Company v. D.B. Modak, 2002 PTC 641

[148] Eastern Book Company v. D.B. Modak, 2002 PTC 641

[149] Lalit Panda, 'The hybridisation of property, liability and inalienability in data protection', 3(2) Journal of Intellectual Property Studies, 18 (2020)

[150] Divij Joshi, 'Non personal data regulation: Interrogating group privacy', Centre for Law & Policy Research Blog, available at < https://clpr.org.in/blog/non-personal-data-regulation-interrogating-group-privacy/> Accessed 26th August, 2020

[151] Tanya Aplin *et al*, 'Gurry on breach of confidence' (1984)

[152] Tanya Aplin *et al*, 'Gurry on breach of confidence' (1984)

[153] Tanya Aplin *et al*, 'Gurry on breach of confidence' (1984)

Some scholars who examine the nature of data as property assignable to a trust argue that under English law, contractual rights, licenses and intellectual property rights may all qualify as subject matters of a trust.[154] They argue that the subject matter of a trust should be viewed as a right attached to property, rather than the property itself. As per this line of thinking, even non-assignable contractual rights can be the subject matter of a trust, as trust law is equally focused on clarifying rights and the duties that go along with rights related to property.[155] However, given that an intellectual property right may not be forthcoming unequivocally for all NPD under consideration, the only way for this to be exercised is if NPD is characterised as assignable to a trust within the bounds of the contractual-obligation of confidentiality.

Additionally, Indian trust law is significantly different from English Common Law on trusts. Specifically, the Indian Trusts Act, 1882 mandates the subject matter of a trust to be "property transferrable to the beneficiary."[156] This phrase has been interpreted to exclude personal rights in relation to property,[157] and this exclusion can also extend to confidentiality based rights.[158] While there is no central public trust statute in India, it has often been held that public trusts will additionally be governed by the principles of the Indian Trusts Act, 1882.[159] Additionally, there is almost no jurisprudence or precedent which interprets any NPD in the context of this definition.

Therefore, in light of (i) the uncertainty regarding whether NPD can theoretically be considered as 'property' for the purposes of a trust; and (ii) the lack of prior jurisprudence in the context of Indian trust law which characterises data as "property transferrable to the beneficiary", there is a significant constraint to operationalising a data trust through the form of a legal trust. Similar concerns about the theoretical validity of trust law for the purpose of data-based trusts have been voiced in other jurisdictions, including various common law jurisdictions.[160] While optimistic legal commentators argue that an interpretation which allows legal trusts to be established for the purpose of establishing a data-based trust is permissible,[161] the lack of any legal certainty on this point creates significant risks in operationalising a data trust through the legal structure of a trust. The possibility of setting up a data trust as a legal trust is not necessarily precluded and may well be tested in a court of law.

## 2. Enforceability of fiduciary duties

Fiduciary duties can be traced within different types of entities which are responsible for the management of a resource. Some examples of this are the fiduciary duty on the trustees of a private or public trust to act in the interests of the beneficiaries of the trust,[162] or the fiduciary duty of a director towards the objects of their company.[163] However, the enforcement of fiduciary duties may not be equally effective across legal structures.

Take for example, the enforcement of fiduciary duties in a Section 8 company. The Companies Act, 2013 has codified the duties of directors of a company – which includes a fiduciary obligation to promote the objects of the company.[164] While a separate penalty is provided for violation of these

[154] Sylvie Delacroix and Neil D Lawrence, 'Bottom-up data Trusts: disturbing the 'one size fits all' approach to data governance', (2019) 9(4) International Data Privacy Law 236.

[155] Ben McFarlane, 'Data Trusts and Defining Property', 29 October 2019, available at <https://www.law.ox.ac.uk/research-and-subject-groups/property-law/blog/2019/10/data-trusts-and-defining-property> Accessed 14 April 2020.

[156] Indian Trusts Act 1882, s 8

[157] Khardah Company Limited v. Raymon & Co, AIR 1962 SC 1810

[158] Tanya Aplin *et al*, 'Gurry on breach of confidence' (1984)

[159] Shivramdas v. B.V. Nerurkar, 1937 39 BOMLR 633

[160] Pinsent Masons et al, 'Data trusts: Legal and governance considerations' (2019), (2020)

[161] Ben McFarlane, 'Data Trusts and Defining Property', 29 October 2019, available at <https://www.law.ox.ac.uk/research-and-subject-groups/property-law/blog/2019/10/data-trusts-and-defining-property> Accessed 14 April 2020.

[162] Pinsent Masons et al, 'Data trusts: Legal and governance considerations' (2019), available at <https://theodi.org/wp-content/uploads/2019/04/General-legal-report-on-data-trust.pdf> Accessed 14 April 2020.

[163] Companies Act, 2013, s 166

[164] Companies Act, 2013, s 166

duties, the specific mechanisms through which these duties can be enforced are not very clear. The enforcement of fiduciary duties has usually taken the form of derivative action suits – which are instituted by shareholders or members of the company against the directors.[165] Commentators have also noted that while the codification of fiduciary duties may have given it a robust theoretical framework, the enforcement of these duties remains suspect.[166] It has also been noted that rarely has a court in India imposed a financial penalty on the directors for breach of their fiduciary duties.[167]

If the mechanisms for enforcement of fiduciary duties appear to rely on derivative action suits, or on claims of oppression and mismanagement, it appears that the enforcement of fiduciary duties is only as robust as desired by the shareholders of the company. Furthermore, an ordinary member of the public would not be able to enforce the fiduciary duties of the director of a section 8 company in the instance that they were acting in a manner contrary to the objects of the company. The lack of a direct mechanism through which ordinary members of the community – all of whom have interests which inhere in the data – can enforce these fiduciary duties is a significant constraint to using these models for operationalising a data trust.

## 3. Competition concerns and market capture by data trusts

Another significant constraint that must be recognised in the operationalisation of a data trust is the scope for market capture by a few early entrants to the setup. Any mechanism which imposes substantial costs on a participating entity would make the operation of a data trust unsustainable – given that at present, the concept is at a very nascent stage and is largely theoretical in nature.

If a data trust is operationalised as an 'umbrella entity' with a limited number of data providers initially on board, then those data providers would be granted influence in shaping the terms of this data trust. This may have direct anti-competitive implications for other data providers. For example, if very few initial data providers can shape the terms of the trust's policies in a manner which privileges existing data providers over new data providers, this may have the consequence of preventing the trust from achieving its desired objective of achieving the public interest.

For example, this constraint and the risk of capture of the data trust is relevant when considering forms in which the governance structure is largely determined by the rules and regulations of its members. Therefore, the rules of an organisation would play a highly influential role in deciding how the society operates, how its policies and terms are framed, and how its membership criteria is defined. The consequence of granting some data providers with a first-mover advantage in these respects is to essentially provide them with excessive control over the participation and rulemaking within a data trust. The direct consequence of this might be the privileging of existing data providers over new data providers.

[165] V Umakanth, 'Director liability under the new regime', Indiacorplaw, available at <https://indiacorplaw.in/2014/06/director-liability-under-new-regime.html> Accessed 26 August 2020.

[166] V Umakanth, 'Director liability under the new regime', Indiacorplaw, available at < https://indiacorplaw.in/2014/06/director-liability-under-new-regime.html> Accessed 26 August 2020.

[167] Mihir Naniwadekar, 'Remedies against Directors undue gains: Personal or proprietary?', Indiacorplaw, available at < https://indiacorplaw.in/2013/09/remedies-against-directors-undue-gains.html> Accessed 26 August 2020

# Evaluating options

The core principles for designing a data trust are identified based on a review of secondary literature relating to data trusts, as well as other similar projects initiated across the world were outlined in Chapter I of this paper. Based on that analysis, it is important to compare the various options for operationalisation of a data trust based on those principles in order to make an informed decision about which legal structure is appropriate for this exercise. The table on the following page conducts this exercise:

| Design Principle | Registered Society | Section 8 company | Public trusts | Summary |
|---|---|---|---|---|
| An enforceable fiduciary duty | A registered society can only be set up for the purposes outlined in Section 20 of the Act. While this places overarching constraints on the exercise of the society's powers, it does not create a trusteeship duty that can be enforced by non-members of the society. | The directors of a section 8 company have a fiduciary responsibility to promote the objects of the company, which can be defined in a manner that conveys trusteeship of a resource. However, this duty is largely enforceable through mechanisms accessible to shareholders only. | The trustees of a public trust have a fiduciary duty to act in the interests of its beneficiaries – however, the lack of any specialised statute which provides the mechanisms for the enforcement of this duty leads to such duty not being enforceable with the same degree of robustness as in a private trust. | The available models do not offer much by way of an enforceable fiduciary duty. In a section 8 company, the fiduciary duty cannot be directly enforced by any ordinary individual. Public charitable trusts, on the other hand, suffer from a lack of robustness in enforceability due to not having a specialised statutory framework. |
| Presence of multi-stakeholder governance schemes | A registered society is largely governed through its rules and regulations, which includes its various byelaws in addition to its charter documents. These rules can provide for multi-stakeholder governance schemes, however, they remain binding only on members of the society. Therefore, this creates a requirement for all stakeholders who wish to be a part of participatory | The Board of Directors of a section 8 company is authorised to create various committees which can provide recommendations to the Board, and such committees can be authorised by the charter documents of a section 8 company as well. These committees can include multiple stakeholders – however their advice ordinarily is recommendatory, as the ultimate responsibility of the Board of Directors is towards the shareholders of the company. | The governance of a public trust is done through the trustees, who are appointed by the settlors of the trust. The terms of the trust deed can provide for these trustees to require consultation with various stakeholders, as well as provide the way the composition of the trustees shall be amended. | It appears that none of the existing models offer an effective multi-stakeholder governance mechanism. The committees formed for a Section 8 company often have recommendatory force. A registered society enables governance insofar as the members of the society are concerned. There do not appear to be effective and clear rules for multi-stakeholder governance in public charitable trusts. |

| | | | | |
|---|---|---|---|---|
| | governance to become members of the registered society. | | | |
| **Sustainability of the repository** | A registered society can enter into contracts, as well as gather commitments of data from its members who have opted into the society. | A section 8 company can develop a sustainable repository through entering into contracts. | The trust deed may permit the trustee to conduct a business or trade, however, if the data is the subject matter of the trust, then any inflow or outflow of data may need to be accounted for in the trust deed. | The sustainability of the enterprise may be safeguarded in each model, however, arrangements with data providers would largely remain contractual, and therefore, the sustainability of the repository would be equally contingent on these contractual arrangements across all models. |
| **Iterative and adaptive systems** | A registered society is only allowed to be set up for the purposes outlined in Section 20 of the Act, which is a constraint on the scope of powers and the purpose of the data trust. The membership of a society is governed by the rules and regulations of the society, and therefore, a degree of flexibility can be provided for in these rules. | A section 8 company can alter its purpose through a special resolution, which requires the approval of the Registrar of Companies. If necessary, it can be converted into a private limited company with the prior approval of the Central Government. While this presents some flexibility of purpose, to continue availing the benefits of being a section 8 company, the data trust would be limited to the 'charitable objects' set out in that section. | A trust deed can be amended to alter the objects of the deed by the board of trustees themselves through a board resolution, or as specified in the trust deed. However, a change to the objects clause may result in a change of the nature of the trust from a 'public charitable trust' to a 'private trust', in which case it shall lose the benefits that it avails due to its charitable nature. | There is a limited degree of flexibility provided by all models, however, any iteration and adaptation is contingent on the members, shareholders or trustees of the entity deciding to revise their charter documents to effectuate any adaptation. |
| **Efficient participation** | Participation in a registered society, including in participatory governance, would require membership of the society. A registered society's rules can require members to pay a subscription to the society, which may increase the costs of participation for them. | Participation in collective governance of a section 8 company would be through participation in the committees that are constituted by the Board of Directors. There are no substantive discernible costs that accompany this participation. | Participation in collective governance of a public trust would be through participation as a trustee. There appear to be no substantial discernible costs that accompany this participation. | While there are potential costs to participation only in a registered society, the degree of participation provided naturally by the other models may not be substantial enough to provide any meaningful influence in the functioning of the entity. |
| **Effective and low-cost** | If any penalty is imposed on any member of a registered society, whether by the byelaws of the society, or by a decision | There are various provisions related to corporate governance which exist in the Companies Act, 2013 for many kinds of conflict resolution – such | In the absence of a specialised statute governing public charitable trusts, conflict resolution relies on suits filed in ordinary courts. Additionally, the lack of a specialised | Conflict resolution with data users would largely depend on the contractual terms, which would be the same across all |

| | | | | |
|---|---|---|---|---|
| conflict resolution | taken at a general meeting, then this financial penalty can be recovered in a court. Litigation proceedings, which would be the primary mechanism of enforcing the byelaws of the registered society, have often been prone to long delays and high costs. | as suits for oppression and mismanagement of the company. The Companies Act, 2013 also provides for specialised enforcement mechanisms such as the National Company Law Tribunal, thereby offering more attractive conflict resolution mechanisms. Given that most data sharing is expected to be contractual in this model, the dispute resolution mechanism that is provided in these contracts or licenses shall govern conflict resolution with data providers or users – thereby enabling more effective and low-cost options than litigation to be adopted. | statute means that the rights and liabilities of various entities are not completely clarified and depend almost entirely on the interpretation of the trust deed – thereby extending the delays and associated costs of litigation. | models. Conflict resolution vis-à-vis the data trust may be better in a Section 8 company when compared to the other models, given the specialised provisions in the Companies Act, 2013 for issues of corporate governance. |
| Graduated sanctions for rule compliance | The sanctions for violation of a rule are determined by the rules, regulations and byelaws of a registered society, which are likely to contain the rules for data sharing amongst members of a registered society. These sanctions can be set out in a graduated manner. | The rules of data sharing in a section 8 company are likely to be contained in the contractual mechanism and licenses that are used by this company. These licenses can adopt graduated sanctions. The sanction for issues related to corporate governance, however, will be as per the Companies Act, 2013 and are unlikely to be graduated. | The contractual rules of data sharing used by a public trust can contain graduated sanctions. The other rules of a public trust will be set out in the trust deed, which may set out graduated sanctions, and would otherwise be governed by the general principles of trust law. | The presence of graduated sanctions depends on the design of the charter documents and the contractual arrangement, which would largely be the same across the three models. |
| Participation in designing collective action agreements | All members of a registered society can participate in the formulation of their rules and regulations. Further, the governing council of the registered society is appointed by all members in accordance with the rules, regulations and charter documents of a registered society. Therefore, there are avenues for participation in the design of collective action arrangements. | Rulemaking in a section 8 company is largely done through the Board of Directors and through meetings of the shareholders. The Board of Directors can constitute representative committees which can provide recommendations to the Board, but the extent of participation in designing collective action agreements will be limited to representation in such committees. | The Board of Trustees makes decisions and rules for the operation of the trust in accordance with the terms of the trust deed. Therefore, apart from representation on this Board, there do not appear to be many other significant mechanisms for participation in designing collective action agreements. | Registered societies seem to provide the greatest degree of participation in designing collective action agreements, however, this would only be for members of the society and not for ordinary individuals. The other mechanisms offer limited avenues for participatory governance. |

| | | | | |
|---|---|---|---|---|
| **Monitoring compliance** | While there is a regulator of registered societies, the powers of this regulator are fairly limited and the violation of the byelaws of the society is generally proceeded against by the members of the society. | There is a regulator for section 8 companies, as well as various approval and transparency requirements, which enable extensive monitoring of its activities. The regulator, that is, the Registrar of Companies, has extensive powers in relation to section 8 companies. Further, the charter documents of a company can place transparency requirements on that company which enable monitoring of its activities by ordinary users. | In the absence of a specialised statute governing public trusts, there are no mechanisms for monitoring of its activities by the ordinary public. The only remedy against a public trust is to enforce the terms of the trust deed in ordinary litigation, however, no specialised mechanisms for monitoring of its activities exist. While the Charity Commissioner plays a role in many states in respect of the registration of a public charitable trust, the exact scope of its powers as a regulator are not clear in the absence of a specialised statute. | The presence of a regulator with extensive powers, numerous transparency and reporting requirements and a sophisticated governance structure make a Section 8 company appear the most robust entity for monitoring compliance, as opposed to the other two entities in consideration. |
| **Regulation of transmission through rules in use** | Transmission of data is done in accordance with the rules, regulations and bye laws of a registered society, which can be enforced under the Societies Registration Act, 1860. The rules and regulations of a society cannot undermine its purpose under Section 20 of the Act, therefore offering an overarching constraint on the substance of these rules. | Transmission of data is done through contractual arrangements and licenses, which can have their own enforcement mechanisms provided for in these contracts. These contracts can generate profits for the section 8 company, subject to the structural limitation that profits should not be distributed amongst the shareholders of the company. Therefore, while there is some regulation of transmission by rules, there is no mechanism which strictly binds these rules to the object of the company. | Transmission of data is done through contractual arrangements and licenses, which will have to be in compliance with the overarching fiduciary duty of a public charitable trust, that is, they will have to be in the interests of the beneficiaries of the trust. | The transmission of data would be done through contractual arrangements across all three models, and therefore, would largely be the same across models. |
| **Nested enterprises** | The rules, regulations and byelaws of a society can provide for multiple sub-committees and other forms of nested hierarchical arrangements which can enable a multi-layered governance structure. | The relationship between the Board of Directors and the shareholders is largely governed through the Companies Act, 2013. However, there are various statutory committees – such as the Audit Committee, the Stakeholder Relationship Committee – as well as other committees which can be established via the charter documents to ensure a nested, multi-layered governance structure. | The Board of Trustees is the single body which is responsible for making decisions about how the asset is utilised. Therefore, there do not appear to be clear mechanisms of organising the public trust as a nested enterprise. | While committees can be formed for a Section 8 company, and a registered society can have sub-committees, neither serve as effective federated structures for the purpose of this principle. |

# Examining the viability of potential options

The table in the previous section compares some of the commonly used structures for registering non-profits vis-à-vis the principles relevant to designing the governance layer of the data trust. Notably, the governance structure of data trusts and similar institutions also depends upon the state of technology used, whereby some design principles can be better adapted based on the technological mechanisms available. Furthermore, there exist various subsidies, benefits and tax-incentives which further impact the effectiveness of such institutions. Before a decision on this issue can be conclusively made, a detailed review of these aspects must be conducted through focused pilots.

On a preliminary analysis, it appears that none of the existing statutory frameworks offer a model that satisfies all of the design principles which are relevant to a data trust. Notably, while public charitable trusts may offer some benefits in terms of an enforceable fiduciary duty, the issues with characterising data as trust property and the lack of a specialised statute raises some concerns about the sophistication and oversight of the governance framework.[168] Similarly, while a section 8 company offers a comprehensive governance framework, the lack of enforceability of the fiduciary duty of the section 8 company by the general public creates a constraint in operationalising a data trust under that structure.[169] Furthermore, the nascent nature of data trusts and low number of early adopters, combined with other issues raised due to the archaic nature of the Registered Societies Act, 1860 raises concerns about competition and capture in relation to the use of registered societies to establish a data trust as a modern cooperative institution.

The lack of compatibility of existing legal structures with a data trust is attributable chiefly to the fact that none of the existing options for operationalising a data trust envisage the creation of structures like a data trust. The laws governing registered societies was conceived of in the year 1860, much before the concept of contemporary data governance. Similarly, while there is no specialised central statute for public charitable trusts, the jurisprudence surrounding trust law has not evolved to clarify the position regarding data as a subject matter of a trust.[170] Consequently, the notions of property which are crucial to trust law are not accommodative of the idea of 'data' as property.

While constraints to establishing data-based enterprises do not exist in the Companies Act, 2013, the purpose of for-profit private limited companies, as well as section 8 companies is markedly different from the idea of a data trust. Section 8 companies are intended to be non-profit companies, which are set up for a public purpose and prevent the transfer of profits to their shareholders.[171] However, they are not envisaged to provide for participatory governance and representative decision-making at a community level. They also lack direct channels through which a member of the ordinary public may enforce the fiduciary duty of the directors of a Section 8 company, given the primacy given to its shareholders within corporate governance.[172]

The evaluation of the various constraints in this chapter, as well as the detailed mapping of various legal structures against the design principles reveals a clear policy gap. While the NPD committee report recommended the concept of a data trust, in order for 'data trusts' to be a reality, legislative and policy measures are necessary to bridge this gap. This would require the development of mechanisms which can enable a specialised governance framework for NPD to be established. Consequently, it appears that legislative and policy measures are necessary which can enable the operationalisation of a data trust in a manner that is true to the design principles identified in Chapter I. The next chapter of

[168] Pinsent Masons et al, 'Data trusts: Legal and governance considerations' (2019), available at <https://theodi.org/wp-content/uploads/2019/04/General-legal-report-on-data-trust.pdf> Accessed 14 April 2020.

[169] V Umakanth, 'Director liability under the new regime', Indiacorplaw, available at < https://indiacorplaw.in/2014/06/director-liability-under-new-regime.html> Accessed 26 August 2020.

[170] Pinsent Masons et al, 'Data trusts: Legal and governance considerations' (2019), available at <https://theodi.org/wp-content/uploads/2019/04/General-legal-report-on-data-trust.pdf> Accessed 14 April 2020.

[171] Companies Act, 2013, s 8

[172] Companies Act, 2013, s 166

this paper, i.e., Chapter IV, sets out some features of this governance framework and offers some recommendations in terms of how this policy gap may be bridged.

However, in order to evaluate the desirability of data trusts, from the perspective of whether they offer an attractive solution to solve some of the issues raised in the NPD committee report, it would be necessary to test whether institutions similar to a data trust are effective in solving these problems. This is also necessary given that the fulfilment of several design principles depends on actual experiences of such an institution based on the context, purpose, composition of the institution, financial constraints and the actual practices and policies devised. To this end, they may be structured as **trusted intermediaries** which are designed to resemble data trusts as far as possible. This would allow an evaluation of the desirability of data trusts from a business perspective and help prototype a governance structure which is true to the optimal idea of a data trust. Practical learnings from these pilots can help advance the state of civil society action on data governance, and are worthy of consideration.

# Chapter IV:

# Bridging the policy gap

This position paper has, so far, analysed the desirability of establishing a data trust, the ideal form of a data trust and considered a strategy for operationalising a data trust. In the previous chapter, the various legal structures which can be used for incorporating a data trust as a legal entity were examined. This analysis revealed that legal structures within the current legal framework – particularly, section 8 companies, registered societies and public charitable trusts – all seem to offer sub-optimal options for operationalising a data trust. Therefore, even though the concept of 'data trusts' has gained currency and is increasingly being considered a desirable model for data governance,[173] the existing legal structures do not appear to be adequate for their establishment.

This situation assumes even greater importance considering the NPD committee report, which suggested data trusts as a governance mechanism for community data.[174] The report, which also proposes significant reforms in the context of governing non-personal data, positions data trusts as a favourable governance mechanism which can help balance the interests of the many stakeholders who would be affected by its wide-ranging recommendations.[175] For data trusts to fulfil this vital role, it is of foremost importance that the requisite legal framework for facilitating their establishment is put in place. Therefore, this part of the paper examines the potential legislative and policy measures which can enable the establishment of data trusts.

## Recognising a bespoke legal entity

The existing legal frameworks do not appear to conceptualise data trusts. This is clear given that most of these statutes look to govern more conventional forms of property and rights, which do not adequately describe the contours of data and data governance institutions like data trusts. The analysis in the previous chapter elaborated on this idea. To effectively allow for data trusts to be established, legislative action which allows for the creation of data-based trusts may be necessary. Attempts to establish data trusts within the existing legal structures will be an exercise of retrofitting these structures to create a data trust, which will inevitably be an imperfect exercise.

Historically, the recognition of new kinds of legal structures and entities has led to the emergence of new forms of commerce and exchange.[176] For example, the recognition of joint stock companies led to the formalisation of many family owned businesses in India, leading to a change in the political economy of trade in India.[177] In the European context, the recognition of joint-stock companies was more transformative, for example. The formalisation of organisations in Europe into joint stock companies enabled projects to be funded by a large, dispersed group of shareholders. This led to the creation of some of the most significant corporate entities of the time and allowed for projects at a larger scale to be funded by a broad base of investors. The proliferation of impersonal

[173] Anouk Ruhaak, 'Data commons & Data Trusts', available at <https://medium.com/@anoukruhaak/data-commons-data-trust-63ac64c1c0c2> Accessed 25th August 2020

[174] Report of the Committee of Experts on Non-Personal Data, Ministry of Electronics and Information Technology

[175] Report of the Committee of Experts on Non-Personal Data, Ministry of Electronics and Information Technology

[176] Nicholas Kyriazis and Theodore Metaxas, 'Path dependence, change and the emergence of the first joint-stock company', Business History, 53(3), 363 (2011)

[177] Umakanth Varottil, 'The evolution of corporate law in post-colonial India: from transplant to autochthony', American University International Law Review, 253 (2016)

exchange driven by joint stock companies has been identified by some to be fundamental to the development of several institutions of modern finance.

While recognising data trusts is similar insofar as it involves the recognition of a new kind of legal entity in the law, data trusts are decidedly set up to be public-centric institutions which enable participatory governance.[178] Therefore, the historical precedent of joint stock companies is relevant to the extent that this is a potentially transformative decision for the political economy of data governance. The direction of this transformation, however, can be designed to be much more commons-oriented and public-centric than the imperatives of joint stock companies.

The recognition of data trusts as institutions for data governance has the potential to transform the political economy of data. In doing so, the legislature is not required to make amendments to existing trust law. It is merely required to create entities for data governance on whom a fiduciary duty is imposed through law. This exercise does not necessarily entail making larger determinations about the nature of data – but instead, involves recognising the narrowly tailored idea that data trusts can be set up as institutions for effective data governance.

# Advantages of a bespoke policy framework

A policy framework enacted to recognise data trusts as bespoke legal entities can be designed in a manner that satisfies the design principles for data trusts that were outlined in this paper. The next section outlines the specific mechanisms which align to each design principle. However, the broad regulatory design of any such policy framework would have the following advantages:

## 1. A specialised registration mechanism for data trusts

Registration of data trusts can accord legal recognition to these entities, without necessarily requiring an overhaul of legal frameworks for section 8 companies, public trusts and registered societies. The registration mechanism can be modelled on the legal frameworks governing companies and registered societies. The formation of a company implies the entry of an entity into the market, and carries with it significant privileges, such as the limitation of personal liability and the power to hold and dispose of property.[179] Consequently, in order for someone to be able to establish a company and obtain these privileges, they are required by law to undergo an incorporation procedure where the Registrar of Companies performs some preliminary checks to ensure the accuracy of information provided by the proprietors of the company.[180]

To foster trust in the ecosystem of data trusts, it is necessary that an entity which wants to call itself a data trust be subject to some foundational eligibility requirements. The registration or incorporation procedure should be straightforward and accessible to ensure that it does not serve as a disincentive to establish a data trust. Additional vetting criteria can form the basis of the data trust being provided additional privileges[181] – such as being able to manage the data for a community,[182] limitations of personal liability and possibly, tax-related exemptions and subsidies.

[178] Anouk Ruhaak, 'Data commons & Data Trusts', available at <https://medium.com/@anoukruhaak/data-commons-data-trust-63ac64c1c0c2> Accessed 25th August 2020

[179] Companies Act, 2013, s 9

[180] Companies Act, 2013, s 7

[181] The procedures and practices ICES Health Data Governance are vetted by the Information and Privacy Commissioner of Ontario (IPC) as a prerequisite for collecting the personal health information of individuals without requiring patient consent. See 'Building Ontario's Next-Generation Smart Cities Through Data Governance', available at <https://computeontario.ca/wp-content/uploads/2019/11/Smart-Cities_ICES_Health-Data-Safe-Haven.pdf> Accessed October 7, 2020.

[182] Report of the Committee of Experts on Non-Personal Data, Ministry of Electronics and Information Technology

## 2. The creation of a competent oversight authority

An oversight authority can help ensure that the data trust is performing as per its objectives and purposes and provide an avenue for community members to raise grievances with respect to the data trusts' functioning.

Currently, the legal framework for entities incorporates a limited form of oversight in addition to the registration procedures mandated. For example, a registered society is required to be registered with the Registrar of Societies.[183] Similarly, a company must be registered with the Registrar of Companies, who also is granted broad oversight powers in relation to companies.[184] Even in the instance of public charitable trusts, the office of the Charity Commissioner exercises some oversight powers over these trusts.[185]

The regulatory and oversight powers required in relation to data trusts are very different from the regulatory powers of regulators under various existing statutes. For example, requiring transparency in terms of data management or processing practices is not a power inherent to the office of the Registrar of Companies. Thus, there is a need to design a bespoke oversight authority specifically keeping in mind the functions of a data trust.

It is necessary to bear in mind the risks of regulatory capture, and the possible existence of a single-point-of-failure for such regulatory capture.[186] Further, the exact nature and composition of this oversight authority is a premature discussion. This is owed to the fact that the concept of data trusts is a very nascent one and will need to be evaluated through several pilots that can provide necessary insight into the functional challenges faced by such entities. Further, challenges in terms of the capacity of personnel, functional independence, and transparency of such regulators must be overcome, which otherwise may result in ineffective enforcement and regulation.[187]

Nevertheless, a few key principles should necessarily guide the development of any such authority:

a) The purpose of the authority should be clearly outlined to benchmark the responsibilities of the authority and hold it accountable.[188]

b) The criteria, qualifications and the processes for appointment and termination of should be transparent[189]. The authority should be competent, comprising personnel with the relevant experience, expertise and market knowledge.

c) The legislative or rule making powers and the process for making rules should be clearly outlined. Additionally, the nature of parliamentary scrutiny must be provided.[190]

d) The procedural powers should be circumscribed by formal procedures with service level assurances and carry the ability to demonstrate adherence to procedures.

---

[183] Societies Registration Act, s 1

[184] Companies Act, 2013, s 9

[185] *See* The Bombay Public Trusts Act, 1950.

[186] Daniel Carpenter and David Moss, 'Preventing regulatory capture: Special interest influence and how to limit it' (2013)

[187] Anirudh Burman, Bhargavi Zaveri, 'How Responsive are India's Regulators', 19 April, 2019, available at <https://www.bloombergquint.com/law-and-policy/how-responsive-are-indias-regulators> Accessed 7 October 2020; 'Regulatory Management and Reform in India, Background Paper of OECD', available at <https://www.oecd.org/gov/regulatory-policy/44925979.pdf> Accessed October 7 2020. Also see, N.K. Singh, 'Regulating the regulators', available at https://www.livemint.com/Opinion/zeVBlQKBAbF9BBx6dQNpWN/Regulating-the-regulators.html (last visited on September 23. 2020.

[188] Shubho Roy, Ajay Shah, 'Building State capacity for regulation in India', Working Paper No 237 (2018), available at < https://www.nipfp.org.in/media/medialibrary/2018/08/WP_237_2018_0ciIwuT.pdf? > Accessed 8 October 2020.

[189] 'The Governance of Regulators, OECD Best Practice Principles for Regulatory Policy', available at <https://read.oecd-ilibrary.org/governance/the-governance-of-regulators_9789264209015-en#page2> Accessed 7 October, 2020.; Shubho Roy, Ajay Shah, 'Building State capacity for regulation in India', Working Paper No 237 (2018), available at < https://www.nipfp.org.in/media/medialibrary/2018/08/WP_237_2018_0ciIwuT.pdf? > Accessed 8 October 2020.

[190] Shubho Roy, Ajay Shah, 'Building State capacity for regulation in India', Working Paper No 237 (2018), available at < https://www.nipfp.org.in/media/medialibrary/2018/08/WP_237_2018_0ciIwuT.pdf? > Accessed 8 October 2020.

At the same time, discretion should be narrow and decision making should be explainable to reduce risks of arbitrary administration and decision-making.

e) The formulation of policies and rules should be consultative.[191] For example, representations by data trusts could be made to a formally appointed consultative committee.

f) Policy and rulemaking should be iterative, subject to regulatory impact assessments at regular intervals.[192]

## 3. Statutory duties and responsibilities of the data trust

The recognition of a bespoke legal entity provides the opportunity for the imposition of duties and responsibilities on a data trust by law. This enhances the enforceability of these duties since they take the form of legal obligations. For example, if a data trust were to be set up as a Section 8 company, many transparency requirements specific to data sharing would be imposed on it by virtue of its charter documents, and not through the Companies Act, 2013. This would mean that the design of the charter documents would be the crucial factor in the imposition of these duties, and the will of its members to enforce the terms of its charter documents would determine the enforceability of those duties. However, when these duties are imposed by law and enforced by an independent oversight authority, they are no longer dependent on the will of the proprietors of a data trust and are mandatory legal obligations on the trust. This fosters accountability in the ecosystem of data trusts.

Similarly, the fiduciary duty of a data trust can be imposed on them through a bespoke policy framework, and this duty can be tailored to the functions of a data trust.[193] Additionally, this duty can be made enforceable by ordinary members of the public who can be affected constituents. Therefore, instead of adapting the fiduciary duty of the directors of a company towards the objects of the company, a specific enforceable duty can be imposed on the entity. The sophistication in regulatory design that is enabled by a bespoke policy framework appears preferable to any retrofitting of existing legal frameworks for establishment of data trusts

## 4. Establishment of mechanisms for participatory governance

The existing legal structures largely lack statutory mechanisms which enable truly participatory governance involving the public in the functioning of the entity. Registered societies are designed to enable collective governance; however, this is only true for the members of that society.[194] Companies and trusts, on the other hand, have limited avenues for participatory governance.

The creation of a bespoke policy framework offers a significant opportunity in this regard. The recognition of data trusts can be accompanied with the recognition of participatory institutions at various federated levels – for example, data users can be enabled to form their own representative organisations which are statutorily recognised within this framework, or organisations at the community-level and neighbourhood-level can be recognised in this framework.[195] The flexibility

[191] 'The Governance of Regulators, OECD Best Practice Principles for Regulatory Policy', available at <https://read.oecd-ilibrary.org/governance/the-governance-of-regulators_9789264209015-en#page2> Accessed 7 October, 2020

[192] Shubho Roy, Ajay Shah, 'Building State capacity for regulation in India', Working Paper No 237 (2018), available at < https://www.nipfp.org.in/media/medialibrary/2018/08/WP_237_2018_0ciIwuT.pdf? > Accessed 8 October 2020.

[193] Larry Ribstein, 'Fencing fiduciary duties', Boston University Law Review, 899 (2011)

[194] Societies Registration Act, s 15

offered to truly accommodate mechanisms for participatory governance when setting up a bespoke policy framework appears preferable to the mechanisms available in existing legal structures.

# Designing a policy framework for data trusts

To design a bespoke policy framework for data trusts, we structure this exercise along the design principles identified in Chapter I of this paper. Therefore, this section examines each design principle, and identifies a mechanism which can fulfil the functions of that design principle.

## I. Design principle: An enforceable fiduciary duty
## Mechanism: Specialised fiduciary duty to be imposed by law on Board of Trustees

- A fiduciary duty needs to be designed keeping in mind the functions and purpose of a data trust. The contents of this duty can involve an obligation to ensure that data is used for purposes which satisfy the public interest, the privacy of the members of the community is maintained and the data trust is not used as a vehicle for private gain.[196]

- The fiduciary duty imposed on a data trust can be imposed on two levels – first, it can be imposed on the entity, where the overall running of the entity and its obligations to the community are outlined; secondly, it can be imposed specifically on the trustees in the data trust, who can be placed under narrowly tailored duties specifically suited to their role. These duties can govern the manner in which the Trustees will perform their activities. Within literature on digital fiduciaries, there are various enumerated duties which can be identified as relevant to the functioning of a data trust and adapted for this purpose.

- A fiduciary duty imposed on a data trust can be made enforceable by members at a community level. This would create a channel for ordinary individuals to be able to enforce these duties, and therefore, would reinstate public agency in the operation of the data trust.[197]

## II. Design principle: Presence of multi-stakeholder governance schemes
## Mechanism: Mandatory composition of sub-committees under the data trust

- The mechanism which can operationalise multi-stakeholder governance schemes is the mandatory composition of sub-committees under the data trust. This can be done in the following manner – where a data trust is sought to be registered or incorporated, the data trust would be required to operationalise some specified committees, such as a data users committee, a data providers committee and a community members committee.[198]

[195] Graham R Marshall, 'Nesting, subsidiarity and community based environmental governance beyond the local level', 2(1), International Journal of the Commons, 75 (2008)

[196] Sylvie Delacroix and Neil D Lawrence, 'Bottom-up data Trusts: disturbing the 'one size fits all' approach to data governance', (2019) 9(4) International Data Privacy Law 236.

[197] Parminder Jeet Singh, 'Data and Digital Intelligence Commons (Making a case for their community ownership), Data Governance Network Working Paper 02 (2019)

[198] Sidney Hirsch and Lawrence Schulman, 'Participatory governance: a model for shared decision making', 1(4), Social work in health care, 433 (1976)

- These committees would, by law, be able to participate in certain decisions of the data trust. The committees can also be granted the power to nominate some members to the Board of Trustees of the data trust, which would provide them with direct influence over the functioning of the data trust. The committees can require membership and take the form of 'closed committees', such as in the case of a data users committee or a data providers committee, and can also be structured as open forums, such as in the case of community members of the committee or for the purpose of specific consultations at a local or sub-local level.[199]

## III. Design principle: Sustainability of the repository
## Mechanism: Commitments by public data providers

- To ensure sustainability of the repository of data, continuous commitments by certain data providers to provide data to the data trust would be necessary. The NPD committee report already takes the first steps in this regard, by conceptualising a power to require the mandatory sharing of some privately held NPD.[200] While the extent of this power, and its desirability in regard to private entities is a larger question, such an obligation can perhaps justifiably be fostered on public data providers.

- Given that public agencies collect their data using means of production which are publicly funded, the argument for mandatory sharing of data in the interests of the community is stronger in this context.[201] The enforcement of this mandate, and the need to ensure safeguards to the use of public data requires state oversight. Therefore, as a first step, the legal framework must grant this power to an oversight authority.

- For privately held data, alternative measures such as compulsory licensing based on FRAND terms, requiring interoperability and specific policy incentives to drive data sharing in the form of tax benefits and enabling access to other data on more favourable terms may also be considered.

- Sustaining the data trust's operations financially will need to be a contextual determination. Several funding models are available to a data trust depending on its legal structure. These include sourcing funds from data providers, data users, the government or other public sector organisations, through philanthropic grants, revenue generation from services provided by the trust, and a combination of all these options.[202]

- For data trusts that are prone to capture, public funding by the State may be considered. Funding from a stakeholder that appears to have financial interests in the data trust should be subject to stricter oversight over their data sharing policies and practices. Revenue generation through license fees charged from data users to sustain the data trusts' operations have been noted to risk a capture by the data steward, particularly where the data trust enjoys a monopoly over that subset of data.[203]

[199] Sidney Hirsch and Lawrence Schulman, 'Participatory governance: a model for shared decision making', 1(4), Social work in health care, 433 (1976)

[200] Report of the Committee of Experts on Non-Personal Data, Ministry of Electronics and Information Technology

[201] Parminder Jeet Singh, 'Data and Digital Intelligence Commons (Making a case for their community ownership), Data Governance Network Working Paper 02 (2019)

[202] 'Data Trusts: Lessons from three Pilots', Open Data Institute (2019), available at <https://docs.google.com/document/d/118RqyUAWP3WIyyCO4iLUT3oOobnYJGibEhspr2v87jg/edit#heading=h.3fngvdcfo2cs> Accessed 8 October 2020.

[203] 'Data Trusts: Lessons from three Pilots', Open Data Institute (2019), available at <https://docs.google.com/document/d/118RqyUAWP3WIyyCO4iLUT3oOobnYJGibEhspr2v87jg/edit#heading=h.3fngvdcfo2cs> Accessed 8 October 2020.

## IV. Design principle: Iterative and adaptive systems
## Mechanism: Periodic review of governance framework and transparency requirements on data trusts

- For the governance framework of data trusts to be iterative and adaptive, obligations on both the government which establishes the broad regulatory framework, as well as on particular data trusts are necessary.

- This can be accomplished by requiring a mandatory periodic review of the governance framework by government committees of experts, who can evaluate whether the governance framework of data trusts is fit-for-purpose and achieving its stated objectives or not. To supplement this exercise, information from data trusts may be necessary since this would provide insights into how the system functions. Therefore, transparency requirements to enable access to this information may be developed in the governance framework.

## V. Design principle: Efficient participation
## Mechanism: Tax subsidies, exemptions, and other benefits

- The costs of participation for various entities in the data trust ecosystem must be justified by the benefits to be obtained. This is particularly important in the context of private data providers, who may see an economic incentive to continue to privately hold their data and prevent its wider sharing.[204]

- While the benefits to the community relative to their costs of participation are fairly obvious (oversight over the use and sharing of community data, prevention of elite capture of community data), and the benefits to the trustees can be in the form of remuneration from the data trust, it is the benefits to private data providers relative to their costs that are a challenging, yet crucial aspects of operationalising data trusts. Therefore, it is proposed that adequate and commensurate benefits can be devised for such entities if they agree to share their privately held data with a data trust.

- Such measures can be determined after undertaking meaningful engagement exercises with the representatives of such private entities, to gauge their interests and inclination in supporting data trusts and working with them. This would help make participation in the data trust ecosystem an attractive proposition.[205]

## VI. Design principle: Effective and low-cost conflict resolution
## Mechanism: Centralised grievance portals, alternate dispute resolution mechanisms and the provision of ombudsman-like powers to the regulator

- The principle of effective and low-cost conflict resolution applies in the context of both data providers, data users as well as ordinary community members. Each of these classes of entities must be able to hold the data trust accountable for its activities, and

[204] Parminder Jeet Singh, 'Data and Digital Intelligence Commons (Making a case for their community ownership), Data Governance Network Working Paper 02 (2019)

[205] Parminder Jeet Singh, 'Data and Digital Intelligence Commons (Making a case for their community ownership), Data Governance Network Working Paper 02 (2019)

the mechanism through which the data trust is held accountable must be effective and low-cost. The various sub-committees constituted under the data trust can also be provided a significant role in conflict resolution.[206]

- As opposed to requiring litigation in courts, which can be a last-resort given its tendency to create delays and raise costs,[207] we propose a combination of the following measures which can enable various entities to hold the data trust accountable.

  - Centralised grievance portals, which can allow for low-cost initiation of complaints with regard to the activities of a data trust. Grievance portals can be operated at the data trust level, as well as at the level of the regulator.

  - Alternate dispute resolution mechanisms, such as mediation and arbitration proceedings, can reduce delays and costs compared to ordinary litigation. These alternative frameworks can also be effectuated through digital frameworks, collectively termed as "online dispute resolution".[208] Typically, ODR mechanisms are gaining rapid popularity for their cost effectiveness, and overall timely resolution of disputes. Such mechanisms can be particularly helpful for resolving disputes at the data trust level between data providers, data users, as well disputes between the data trust and users and providers, respectively.

  - The oversight authority should also be provided ombudsman-like grievance redressal powers in relation to the activities of the data trust. This would enable for a level of appeal from the grievance redressal mechanisms of the data trust and would not require litigation to be the only available alternative for an aggrieved entity.

## VII. Design principle: Graduated sanctions for rule compliance
## Mechanism: Sophisticated formulation of sanctions for data trust and data users

- The legal framework governing data trusts can provide for sophisticated sanctions, applicable to the data trust, the data providers as well as data users who violate the terms of data sharing.

- For example, in relation to end-users, a series of sanctions – ranging from terminating their access to the data via API streams, imposing financial penalties and initiating legal proceedings – can be developed in the instance that they are found violating the terms of data sharing.

- Similarly, in relation to the data trust, sanctions ranging from providing financial compensation to aggrieved community members or organisations, requiring the disqualification of various trustees from participating in the data trust ecosystem, imposing injunctions on the use of certain technologies, to the initiation of criminal proceedings (in certain cases) against the trustees, can be considered.[209]

[206] Sidney Hirsch and Lawrence Schulman, 'Participatory governance: a model for shared decision making', 1(4), Social work in health care, 433 (1976)

[207] ODR: The Future of Dispute Resolution in India, Report by the Vidhi Centre for Legal Policy, available at < https://vidhilegalpolicy.in/research/the-future-of-dispute-resolution-in-india/> Accessed 26th August, 2020

[208] ODR: The Future of Dispute Resolution in India, Report by the Vidhi Centre for Legal Policy, available at < https://vidhilegalpolicy.in/research/the-future-of-dispute-resolution-in-india/> Accessed 26 August, 2020

[209] 'Data trusts: lessons from three pilots' Open Data Institute (2019), available at < https://docs.google.com/document/d/118RqyUAWP3WIyyCO4jLUT3oOobnYJGibEhspr2v87jg/edit#heading=h.tmv9fe212sd1 > Accessed 8 October, 2020.

## VIII. Design principle: Participation in designing collective action agreements
## Mechanism: Participative governance structures and processes

- For formulating the broad policies of the data trust, consultation with the data users, data providers and community members committee should be mandatorily required. If the data trust wishes to make a specific policy regarding data at a sub-local level, for example, then consultation at that level specifically can be required. The format for local and sub-local stakeholder consultations can be defined.

- Formation of federated committees will enable this process and make it practicable for a data trust to involve data providers and data users within the decision-making process. For this, various sub-committees should be mandatorily constituted under a data trust, such as the data users committee, the data providers committee and the community members committee, can be provided specific roles and entitlements which are granted to them by law. For example, the right to nominate members to the Board of Trustees, the requirement that any policy of the data trust shall mandatorily require consultation with these committees in a defined format, and the principle of subsidiarity in participatory governance[210] – that is, policies for specific areas or sub-divisions shall be formulated in specific consultation with the members of that area or sub-division, can ensure that there is participation in designing collective action agreements.

- Direct citizen participation through accessible avenues – such as through mobile phones – must be integrated by data trusts through public consultations, providing a designated forum for citizen participation, ensuring informed participation by publicising public information that is clear and comprehensible to a citizen. The data trust may also engage local collective governance frameworks such as residents' welfare associations, municipal corporations, and local panchayats, local consumer and civil society organisations to ensure citizen participation.

- Government initiatives in this regard include running information campaigns, ensuring local representatives and relevant government departments participate in the decision-making process to reflect community interests, and work towards building the capacity of data trusts in integrating the participation mechanisms discussed above. In some cases, local governments have tied up with local civil society organisations to run capacity building campaigns that train individuals to use the technology used to collect data in community data governance pilots.[211] Public assessment of proposals may also be conducted through independent review boards comprising various stakeholders that provide focused expertise required for such assessment.[212]

- More sophisticated means such as blockchain based community management can be evaluated more deeply at a later stage

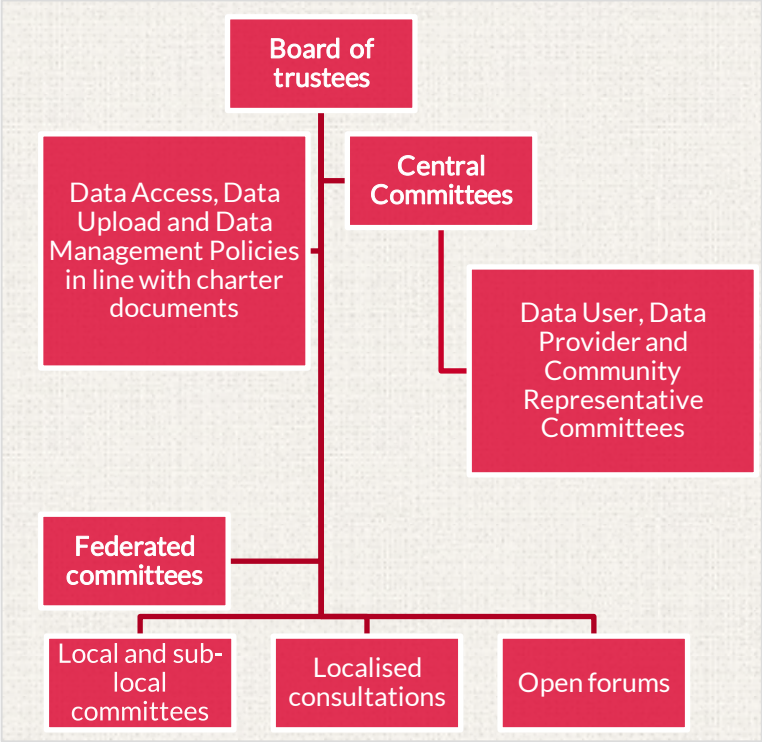
[210] Robert K Vischer, 'Subsidiarity as a principle of governance: beyond devolution', 35 Indiana Law Review, 103 (2001)

[211] See the DECODE Project in Barcelona, which set up a community-based data governance framework, where city residents were provided training to understand how to use sensors involved in collecting data in the project. This was carried out in collaboration with local community organisations. See Oleguer Sagarra, Xavier Hoffmann et al, 'Final report on the Barcelona Pilots, evaluations of Barcelona Now and sustainability plans', Project DECODE (2019), available at < https://decodeproject.eu/publications/final-report-barcelona-pilots-evaluations-barcelonanow-and-sustainability-plans> Accessed 7 October, 2020.

[212] The Surveillance Advisory Working Group in Seattle conducts civil liberties and privacy assessment of surveillance technology proposals. See 'Surveillance Advisory Working Group', available at < https://www.seattle.gov/tech/initiatives/privacy/surveillance-technologies/surveillance-advisory-working-group> Accessed 8 October 2020.

as blockchain-based technology evolves and the data trust market matures.[213]

- The diagram on this page contains a representative illustration of the governance structure of a data trust, which is designed to ensure efficiencies in sharing of data while safeguarding participatory governance through mechanisms such as various representative committees, localised consultations and creation of open forums at local and sub-local levels.




## IX. Design principle: Monitoring compliance
## Mechanism: Transparency requirements and designation of an oversight authority for data trusts

- Accountable monitoring demands that the actions of the data trust be monitored, and the oversight authority be accountable to the public and the community. To actualise this principle, obligations on both the data trust as well as the oversight authority would be necessary.

- Monitoring of the compliance of the data trust with the provisions of the regulatory framework, as well as with its own policies, required transparent disclosures as a pre-requisite. Transparency mechanisms include periodic audits, disclosures of data usage and sharing, in addition to financial statements, accounts and other reports which can help make the functioning of the data trust visible to members of the community.

- Certification mechanisms, either prescribed through standard formats or developed by the oversight authority, can ensure best practices are followed. Certification can also convey to the public whether a data trust is functioning in a trustworthy manner or not.

- The oversight authority, on the other hand, can be designed in a manner where there is transparency in the appointment of its members as well as their functioning. Further, the sub-committees under the data trust may be provided a right of audience with the authority in a defined format, which would enable the oversight authority to be accountable to the members of the community as well.

[213] Risto Karjalainen, 'Governance in Decentralised Networks' (2020), available at <https://streamr-public.s3.amazonaws.com/governance-whitepaper-2020-05-21-v1_1.pdf> Accessed 8 October 2020.

## X. Design principle: Regulation of transmission through rules in use
## Mechanism: Publicly available policies and technological systems to regulate data flows

- The data trust should be required, by law, to formulate and make publicly available policies related to:

  - Data access policy, which would set out the terms and conditions to be followed by the users in accessing the data sets. This may include standard terms of use, the options for licenses which may be used, retaining the right to audit the use of data, termination terms laying out data obfuscation requirements and other terms related to accessing the data trust's platform
  - Data upload policy, which would govern the formats of data that are shared with the trust, require undertakings related to anonymisation and integrity of data from data providers and prescribe various standards related to the data which can be shared with the trust.
  - Data management policy, which would specify the security standards, internal access policies, anonymisation standards and other responsibilities of the data trust in relation to the data. The policy should also specify the manner in which access to certain data may be terminated or archived as a consequence of the expiry or termination of the license, as well as the winding up of the data trust.

- The legal framework can set out some standards which the above-mentioned policies must adhere to, thereby ensuring a minimum level of protection for the interests of the community. The licenses through which a data trust shares any data can be required to be made publicly available, in order to enhance transparency in its functioning. Solutions which can technologically address issues related to the flow of data and participation in decision making may be considered.
- This study specifically looks at data trusts as a solution for trusted sharing of NPD. Thus, the rules in use should specifically exclude personal data sharing if the purpose of the data trust is to govern NPD. This is because personal data sharing requires additional obligations requiring prior consent and warranting stricter controls over its use.

## XI. Design principle: Nested enterprises
## Mechanism: Identifying participants and their roles in the data management process.

- As stated above, the data governance under a data trust will entail some level of government oversight. At the first instance, the proposed registration and oversight authorities will provide overarching rules to enforce data management policies, provide policy guidance to data trusts and over time develop standards for collective data governance.

- In cases where public data is the subject matter of a data trust or involves data pertaining to public functions, the concerned government department or agency, and the appointed data security officers will be key participants in this framework. For instance, where municipal level smart city data is concerned, the relevant urban development

ministry as well as their data custodian can form part of the governance framework.[214]

- Within the data trust, the sub-committees of a data trust should not be centralised committees which serve as exclusive conduits for participatory decision-making.[215] While the creation of these committees is the first step towards enabling a nested enterprise, these committees should further be required to have federated sub-divisions at various levels.

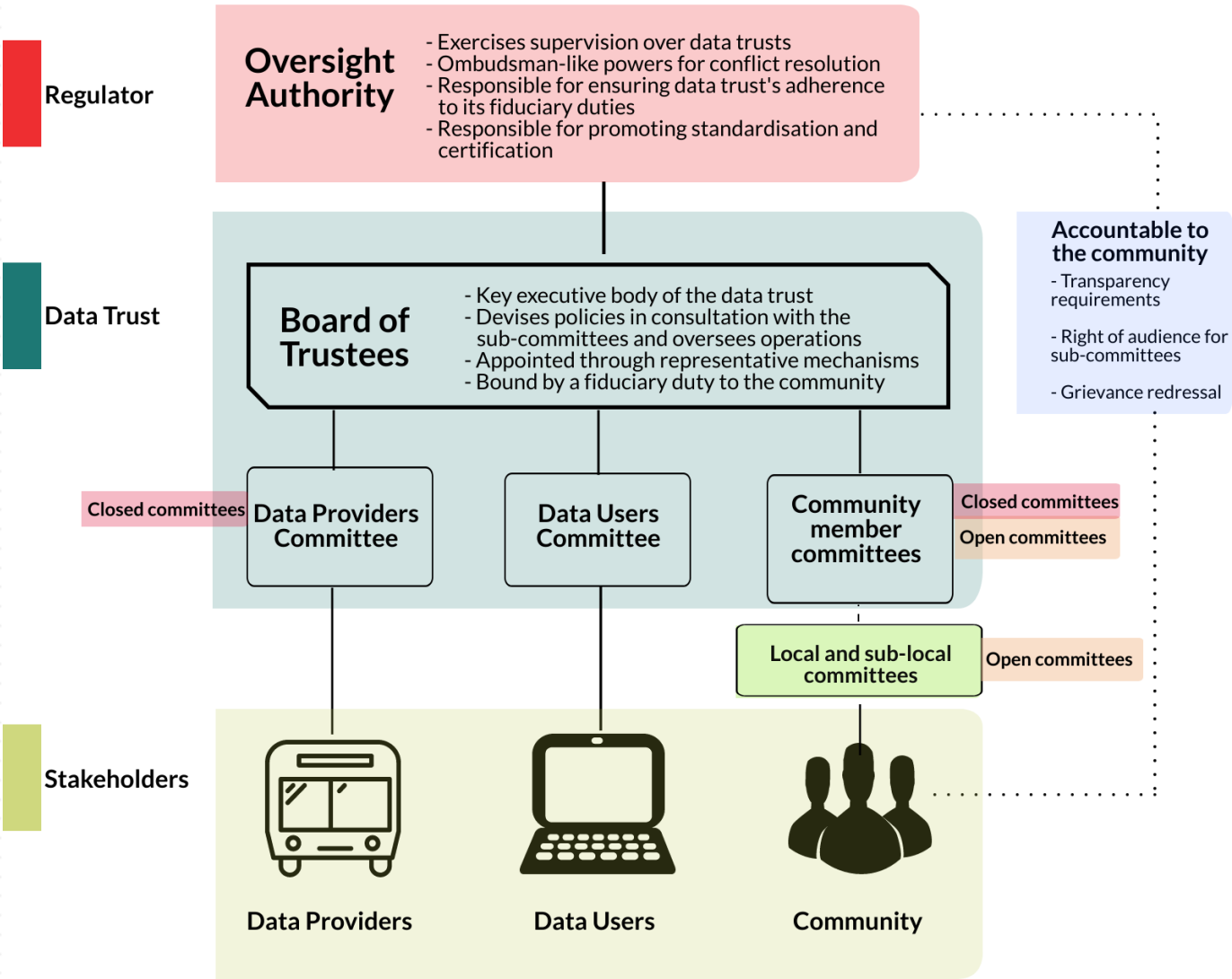
- In the context of data commons, entities like standard setting bodies also play a key role in nudging the market towards best practices. Existing security and data management standards set by such bodies can be further revised through engagement with data trusts and the oversight authorities in this space.

[214] Natalie Chyi and Yuliya Panfil, 'A commons approach to smart city data governance', New America Foundation (2020), available at < https://www.newamerica.org/future-property-rights/reports/can-elinor-ostrom-make-cities-smarter/> Accessed 7 October, 2020.

[215] Sidney Hirsch and Lawrence Schulman, 'Participatory governance: a model for shared decision making', 1(4), Social work in health care, 433 (1976)

# Key aspects of the regulatory framework

Based on the above discussion, the following blueprint provides an illustration of how a data trust may be designed and how such a design is likely to function:




Based on this model of establishing data trusts, it emerges that the regulatory framework which is established for data trusts would have the following key characteristics:

## I. Registration mechanism

- A registration mechanism, where certain preliminary checks to ensure the credibility of the data trust is conducted by an oversight authority may be developed.
- A data trust wishing to be registered as such can apply for this registration, which may be tied to a set of privileges or incentives.

## II. Board of Trustees

- A data trust should be required to have a Board of Trustees. There should be prescribed eligibility criteria for someone to be a member of the Board of Trustees. This mechanism may potentially evolve into an empanelment mechanism for appointment of members to the Board of data trusts.
- Further, rules enabling sub-committees of the data trust to nominate members to the Board of Trustees should be framed to enable participatory governance. These rules can set out the number of sub-committees and their manner of composition, the open/closed nature of the relevant sub-committees and develop an institutional structure for interaction between the Board of Trustees and the sub-committees of the data trust.

## III. Sub-committees of data trust

- A data trust can mandatorily be required to formulate at least three sub-committees: a data users committee, a data providers committee, and a community members committee – which may be required to necessarily be an open committee. These committees should be provided clearly defined roles and responsibilities in relation to the operation of a data trust.
- The sub-committees should have the right to nominate members to the Board of Trustees, be mandatorily consulted in the formulation of the data trust's policies and have the right of audience with the oversight authority in a defined format.

## IV. Federated sub-committees

- The sub-committees should also be developed in a federated manner, with specific sub-divisions, based on either geographical area or other considerations. These sub-divisions of sub-committees should have clearly defined roles in relation to the larger committee and the data trust, as well as decision-making privileges in relation to some activities which particularly affect the sub-division.
- If a policy which specifically affects any sub-division is formulated, then the members of that sub-division should have a privileged right of consultation in relation to that policy, which can be operationalised by taking practical steps to consult the community at a local or sub-local level.

## V. Fiduciary duty of data trust

- The data trust shall have fiduciary duties on two levels: the entity itself shall be responsible for certain kinds of duties, and the Board of Trustees shall have narrowly tailored duties adapted to their functioning.
- These duties should be enforceable by ordinary members of the community, as well as by any of the sub-committees or the oversight authority through effective and low-cost mechanisms.

## VI. Policies of data trust

- The data trust can be required to have some publicly available policies which set out the manner of its functioning.
- The regulatory framework should establish minimum standards in relation to these policies, which shall ensure the protection, enhancement and promotion of the public interest.

## VII. Transparency requirements for data trusts

- The data trust should be imbued with various transparency requirements in relation to its functioning, which can be developed to ensure trust in its operation and monitoring of its compliance with the regulatory framework as well as with its own policies.

## VIII. Conflict resolution mechanisms and sanctions

- The data trust should have grievance redressal portals at two levels – at the level of the data trust, as well as the level of the oversight authority. The oversight authority can also be imbued with ombudsman-like powers, which enable it to be a forum for conflict resolution.

- Online dispute resolution mechanisms can mandatorily be required of the data trust. Additionally, the sub-committees of the data trust may be granted a right of audience with the oversight authority in a defined format.

## IX. Oversight Authority

- An oversight authority may be established, which shall have powers in relation to registration of data trusts, supervising their operation and acting as a node in conflict resolution.
- The oversight authority may also be provided the power to require commitments from public agencies for mandatory sharing of their data with data trusts, in order to make the data trust ecosystem sustainable.

## X. Powers and duties of Oversight Authority

- The oversight authority may be provided with supervisory powers over data trusts, as well as the ability to impose various sanctions on data trusts for violation of the legal framework or their own policies.
- The authority should be constituted in a transparent manner, and have various mechanisms which improve the accountability of the regulator, such as requiring disclosures, performance reports and providing sub-committees of data trusts a right of audience with such regulator in a defined format.

# Conclusion

I. The concentration of data and digital intelligence in a few successful companies is a symptom of a digital economy that lacks institutional structures for the exercise of collective rights and community interests in data. Particularly in the context of NPD, there is a need to ensure that institutional arrangements which can provide the mechanism for exercise of community interests in data are devised.

II. The polycentric nature of NPD and the many varied, and often competing interests which inhere in this data are required to be balanced in a manner that achieves the public good. This paper posits that a governance solution in the form of data stewardship can address these issues by creating an institutional framework through which citizens and other stakeholders can exercise control over NPD.

III. The existing state of the digital economy indicates that an institutional innovation, such as a stewardship-based solution, can help reorient data governance towards the public good. In order to develop a stewardship model for this purpose, we examine existing literature on common-pool resources and resource commons (such as natural resource commons and knowledge commons) to analyze the potential forms that a data commons for NPD may take.

IV. This paper identifies eleven design principles based on existing literature on resource and knowledge commons, which have been adapted to the particular context of the digital economy. This draws from pioneering work on structuring knowledge commons and sets out a coherent system of principles vis-à-vis which any stewardship solution can be assessed.

V. Based on this evaluation, the paper posit data trusts as model of data stewardship that may be best-placed to achieve the objectives of effective, public-interest oriented data governance, whereby the community members are included within the data management process and enforce their rights through an actionable fiduciary duty.

VI. The paper proceeds to examine whether such a data trust can be established under the existing legal framework in India. After analysing various non-profit legal structures against the design principles for a data commons, it finds that the current legal paradigm does not support the setting up of data trusts in a manner that guarantees that each of these principles is fulfilled in spirit and practice.

VII. The establishment of data trusts at this stage requires several regulatory and policy interventions that can address the shortcomings of each of the legal structures studied. At the same time, some aspects of data governance under a data trust will become clear primarily through pilots set up across different contexts, which can be established to evaluate the benefits of such institutions.

VIII. With respect to the regulatory and policy interventions foreseeable at this stage, we propose a bespoke framework catering to data trusts, comprising obligations for both the government as well as data trusts as they are established. These are summarized below:

# Recommendations for data trusts

I. Data trusts should be incorporated as multi-layered organisations, with federated sub-committees and sub-divisions, which have clearly defined roles, to represent various stakeholder interests.

II. A board of trustees should be appointed, and sub-committees need to be clearly outlined for each representative group, as well as at the local and sub-local level. The appointment of each should be transparent, based on defined eligibility criteria. At the same time, direct avenues for participation such as online fora, community meetings, engagement with local governance bodies and civil society organisations can be required in respect of local and sub-local consultations.

III. The data trust should have an enforceable fiduciary responsibility to protect the public interest and safeguard community interests in data. These duties should be directly enforceable by the community members and the representative sub-committees.

IV. The data trust can mandatorily be required to share information regarding their internal policies, as well as periodic disclosures regarding their functioning, such as the status of repositories managed, an audit trail for its use of data and its financials.

V. Mechanisms need to be developed to resolve conflicts between the participants of the data trust, as well as to enforce the duties to the public. For the former, the online dispute resolution mechanisms can be mandated.

# Recommendations for government intervention

I. The review of existing legal frameworks for the specific context of data create several spillovers for other sectors. This requires a deeper review of these frameworks, which may not be feasible. Instead, a registration mechanism and a bespoke policy framework, to recognize data trusts as legal entities can validate their legal status based on minimum eligibility criteria.

II. While a data trust is expected to be a community-first entity, an oversight body is necessary to ensure that data trusts remain true to their purpose and carry out their functions as per the expected code of conduct.

III. The powers and functions of such a body must be clearly outlined, and the body should be set up to ensure its functional independence to minimize any government bias. At the same time, the body should be driven by evidence-based decision making and iterative policymaking based on periodic reviews.

IV. The state oversight function should also be accompanied by obligations to encourage standardization and adoption of such standards through incentive frameworks and certification requirements.

V. The oversight authority should be granted ombudsman-like powers to provide a specialized avenue for redress of grievances. The ombudsman should be obligated to function transparently and within a time-bound manner.

VI. Apart from direct intervention through oversight and registration, the state must also undertake capacity building efforts to ensure informed participation of communities in the data management framework under a data trust and promote the adoption of new technologies that can support data trusts in community-based data governance.

# Issues to be resolved through pilots

I. A data trust may be financed through several avenues, including through stakeholder contributions, state and private grants, revenue generation through its activities, etc. However, accompanying risks of monopolization of resources, biased decision making and limits to scaling up need to be evaluated for each data trust based on the stakeholders involved, the type of data being stewarded, the available government or private resources, etc. Pilot exercises are needed to evaluate these risks and develop solutions.

II. There is a need to assess the types of incentives that can ensure a continuous supply of data to the data trust. While a public sector entity may be mandated to share data, private entities and organisations are likely to require specific incentives in the form of tax deductions, waiver of specific conditions in obtaining state licenses and registrations for their respective activities and other such incentives.

III. Pilots for specific sectors – such as urban mobility data – can provide experiential insights into the viability and success of data trusts. This would also involve negotiating practical rules, conditions and complex relationships between different stakeholders. Outputs from such Pilots can provide a useful tool for advancing the conversation on data trusts.