Trust Law, Fiduciaries, and Data Trusts

by
Siddharth Manohar

THE DATA ECONOMY LAB

The Data Economy Lab is a partnership between Aapti Institute and Omidyar Network India

Acknowledgements

The author is grateful for the valuable insights and contributions of Nikita Agarwal, researcher at the Oxford Internet Institute, Keith Porcaro, founder of independent data governance consultancy Small Scale, and colleagues at Aapti Institute.

Contents

I Introduction

This article looks at the use of trusts in data governance. It starts with a discussion of data trusts—it covers questions of what data trusts are, how they operate—what makes them useful tools, and the legal structures underpinning them—whether there is always a legal trust in association with a data trust. The article explores these questions by diving into specific formulations of data trusts in certain jurisdictions, namely the UK and India. Approaches in each of these countries have been shaped differently in regulatory structure and experimentation.

The problem with data governance remains that of finding means of ensuring compliance. Companies violating contractual terms, such the agreed purposes for use of data, or changing terms of sharing without adequate user notice, in the current context need to be taken to task by individual users or companies who are harmed by such violations. If there is no individual entity or person harmed by the violation, the companies are not directly answerable to an authority; the exception to this being specific violations of data protection laws in certain jurisdictions.

II Data Trusts as a Solution to misuse of data

The data trust is a form of data governance where an entity is appointed to hold data "in trust" on behalf of a certain set of beneficiaries.[1] This framework can vary in its constituting elements according to the context in which it is established. For instance, a set of users coming together to pool their data may appoint a trustee from amongst them, or even an external one. Another example may involve a company with a large dataset on its users establishing a relationship with a data trust, external to the company, for the data to be used for research.

In both instances however, the data trust operates as a steward of the data, an entity given certain responsibilities to protect user interests, such as to regulate data usage according to permissions granted by the user, and to curate the third parties with whom the data is shared, according to the purpose for which the data trust has been set up.[2]

The idea of data trusts draws on the common law concept of a trust. A trust consists of a legal arrangement wherein a person authorises an individual or entity to manage certain property for the benefit of a third party or for certain defined purposes. In the context of data, the trust is tasked with protection of the interest of users and managing the data accordingly. For example, a data trust sharing data with a third party would ensure encryption and purpose restrictions as specified by its policies before and during the course of sharing access to data.

1 Sylvie Delacroix & Neil Lawrence, "Bottom-up data Trusts: disturbing the 'one size fits all' approach to data governance", International Data Privacy Law, Volume 9, Issue 4, 2019, accessible at https://academic.oup.com/idpl/article/9/4/236/5579842/.

2 Mark Bunting & Suzannah Lansdell, "Designing decision making processes for data trusts: lessons from three pilots", Office for Artificial Intelligence of the Government of the United Kingdom, 2019, accessible at http://theodi.org/wp-content/uploads/2019/04/General-decision-making-report-Apr-19.pdf.

III Why do Data Trusts make sense?

To understand why the concept of a trust is suitable for the purpose of handling data, it is useful to look at its constituting principles. Classically, trusts consist of a notional transfer of title over a property to a person (known as the trustee) who is legally obligated to use the property to fulfill certain obligations—often for the benefit of a designated person, known as the beneficiary. Applying this logic to the data economy, the property here would seemingly take the form of data, the beneficiary end users, and the trustee(s) the entity set up as the data trust. Interestingly, a legal report commissioned on the question by the Open Data Institute[3] categorically states that the legal vehicle of a trust is not suitable to an entity to manage user data—so why has the data trust gained traction?

In the context of data being leveraged for public as well as private purposes, a balance needs to be found between user interests and benefits to other stakeholders looking to use data. Protection of user interests until now has chiefly taken the shape of explicit legal regulation, specifically data protection regulations, in a number of jurisdictions. In India, the draft Personal Data Protection Bill[4] (PDPB) awaits passage in Parliament, while the government has also made mention of the use of data trusts in the Report on Non Personal Data.[5]

These regulations make attempts to protect users either through sectoral regulation or hard law by prescribing how data should be handled across the board. Sectoral regulations by their nature suffer from only being applicable in the area for which they are designed. Legislation applicable across the board on the other hand, while necessary, lacks the specifics and nuance that may be required while looking at managing the use of data in different purpose-specific contexts. This shortcoming may also be faced by sectoral regulations, which can only lay down rules, and may not

3 "Data trusts: legal and governance considerations", Pinsent Masons & Ors., 2019, accessible at https://theodi.org/wp-content/uploads/2019/04/General-legal-report-on-data-trust.pdf.

4 "The Personal Data Protection Bill", 2019, Ministry of Electronics and Information Technology of the Government of India, accessible at http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.

5 "Report by the Committee of Experts on Non-Personal Data Governance Framework", Ministry of Electronics and Information Technology, accessible at https://ourgovdotin.files.wordpress.com/2020/07/kris-gopalakrishnan-committee-report-on-non-personal-data-governance-framework.pdf.

direct the actual operation of data sharing and management. This leaves a void of an actor, or an agency, which is capable of recognising the potential harm to user interests and the public.

IV The Role Of Data Trusts

The data trust plays the role of a body that oversees data sharing and usage practices. As a steward tasked with intermediary responsibility over data, it is better placed to enforce ethical obligations on data use and take direct measures against violations, including public notice and termination of access to data.

In order to play an oversight role, the data trust needs to draw its authority from users. This could be through a collective of users coming together to create a body to govern the usage of their pooled their data; it could be formed through appointment by contract or by an authority.[6] The specifics of the form and practices of a data trust may vary according to the purpose and the sensitivity of the data that it handles—public data on pollution levels and statistics for example, would require less scrutiny over management practices than data that may be able to identify sensitive details about individuals.

The central credit to this system is the existence of an entity that acts as a manager of data usage and sharing practices, and represents the users and companies providing this data. Current value chains of data sharing do not allow for user agency to find any meaningful representation in decisions on how data is used. The existence of the data trust is intended to hold third parties accountable to their stated purpose and extent of data usage. This makes it possible to protect user interests whilst managing the relationship between disaggregated third parties and masses of users from whom the data has been collected.

The defining currency of this system however, remains trust (in the conventional interpretation of the term) and accountability. 'Data trusts' need to build trust in their services in the minds of stakeholders through the implementation of effective accountability mechanisms. Part of this involves allowing users to choose form a wider set of preferences in how their data is used and shared. Increased negotiation power to realize their

6 "Extended ODI Data Trust report: Further use cases to consider", BPE Solicitors, 2019, accessible at http://theodi.org/wp-content/uploads/2019/04/BPE_PITCH_EXTENDED_ODI-FINAL.pdf.

preferences is part of this, along with the access to the necessary tools to do so. Better enforcement of rights, increasing portability between services, all of these measures contribute to increased user autonomy, which forms one of the chief aims of increasing accountability and trust in the data economy.[7]

7 Sylvie Delacroix and Neil Lawrence, "Bottom-up data Trusts: disturbing the 'one size fits all' approach to data governance", International Data Privacy Law, 2019, accessible at https://academic.oup.com/idpl/article/9/4/236/5579842.

V The Property-led Model of Control over Aggregated Data

The currently posited model of data governance puts operational power in the hands of the data processor, with rights-based restrictions on their actions. These restrictions follow a pattern of protection of individual interests in data, similar to protection of interests in property.[8] It inheres in individuals certain inalienable interests in personal information, which provide the principled basis for control over the actions of third parties who access this information.[9] Third party access itself is conducted on the terms consented by the individual. This restricted form of access too is derived from property assignment, where certain restrictions are attached to the assignment of rights to access the data. Extended implementation of user control and consent is a challenge for third parties however—tertiary data transfer transactions would bear a high cost for obtaining direct user consent. This was also demonstrated in instances such as the Cambridge Analytica incident where large quantities of data were accessed without user consent.[10]

This led to a rethinking of the nature of the duty of data processors, with the idea of a fiduciary obligation on them coming to the fore.[11] Fiduciary responsibility has been seen as a solution to this conflict of interests, placing broader restrictions on the data processor to prohibit acting against the interests of end users. Fiduciary responsibility places a higher burden on data processors to act in good faith and in the interests of users whose data it controls. This also results in clear legal liability of the data processor in case of violation of this duty.

8 Jacob Victor, "The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy", Yale Law Journal, 2013, accessible at https://www.yalelawjournal.org/comment/the-eu-general-data-protection-regulation-toward-a-property-regime-for-protecting-data-privacy/.

9 Paul M. Schwartz, "Property, Privacy, and Personal Data", Harvard Law Review, 2004, accessible at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=721642.

10 "Prof. Jack Balkin on Facebook and the Risks of 'Data Capitalism'", Yale Insights, 2018, accessible at https://insights.som.yale.edu/insights/three-questions-prof-jack-balkin-on-facebook-and-the-risks-of-data-capitalism/.

11 Jack M. Balkin, "Information Fiduciaries and the First Amendment", UC Davis Law Review, Vol. 49, No.4, 2016, accessible at https://lawreview.law.ucdavis.edu/issues/49/4/Lecture/49-4_Balkin.pdf.

VI Usage of Trust law in Data Fiduciaries

The usage of the term "trust" or "fiduciary" as in the case of data fiduciaries, when seen using the PDPB and the GDPR as markers for legislative frameworks, prove as misnomers of a kind. Until now the use of Trust law has remained a theoretical basis, its appeal in the use of fiduciary duties and trusteeship to enforce on data processors duties that protect the interests of users.

The PDPB, while circumscribing the extent and forms in which a company may deploy user data and share said data, does not require the company to act in any set of interests other than its own. This is contrast to the core idea of legal trust and fiduciary responsibility, where the trustee (ie the fiduciary) is required to act in the interest of the beneficiary (in this case the user). The only instance where this principle finds mention is in the section of the Bill that deals with children's data. The fact that it puts forward the principle in this section and leaves it thereby conspicuously absent in the general provisions of the Bill, makes it clear that the Bill does not conceive of the relationship between the data 'fiduciary' and the user as one of actual trust placed in recipient of the property.[12]

It has also been observed that part of the discussion on the notice and consent regime of data sharing in the wider world has been inadequate as a legal and policy structure to prevent the misuse of user data. It is for this reason that solutions such as Data Trusts are now in the spotlight. However, the analysis laid out now indicates that there is the lack of a proper fiduciary framework adopted by the law. In its stead is a set of requirements on notice, restrictions on processing, and consent rules in place to prevent harms to users arising from data processors.

Jack Balkin, the foremost contemporary thinker on information fiduciaries, argues that the right of these companies to hold data rests on their responsibility to use data in a manner that does not abuse the

12 Rishab Bailey and Trishee Goyal, "Fiduciary relationships as a means to protect privacy: Examining the use of the fiduciary concept in the draft Personal Data Protection Bill, 2018", Data Governance Network Working Paper, 2019, accessible at http://datagovernance.org/files/research/NIPFP_Rishab_Trishee_fiduciaries_-_Paper_4.pdf.

trust placed in them by users.[13] The operative commercial and legal understanding of data processors entrusted with data does not go as far as the concept as put forth by Balkin, whose thesis requires information fiduciaries to take cognizance of the harms of their data processing not only on the individuals they may be contracted to (albeit in many cases in a limited sense under the terms of the service provided), but rather to society as a whole. The fiduciaries owe a duty of care and loyalty to users. As a matter of practice, legal frameworks do not account loyalty to user interests, and often assume the contrary. The duty of care however has been implemented through legal requirements of consent, purpose limitation, and other restrictions, along with penalties for violation of these provisions.

This idea of information fiduciaries has since been expanded, with further light on different extents of fiduciary responsibility. One level of fiduciary responsibility would be that of making sure that there is no harm to users from the actions of the information fiduciary itself. The other form of fiduciary responsibility is a higher threshold where the information fiduciary takes active measures to protect the rights and maximize the interest of the users in its trust.[14]

Part of creating the solution for fiduciary responsibility to be useful to users seems to be a mix of the public and the private—there is increasing consensus that each on their own has different problems. A purely top down approach of regulation stifles what digital service providers feel they can do in the market, and private platform for redressal depend on nonexistent standards of digital literacy and user-led negotiation power. A combination of both therefore, is the only approach that stands a chance of plugging these gaps. Providing a platform for users to exercise control is ostensibly useful and pragmatic, but this measure needs the statutory support of fiduciary responsibility placed on actors who are invested with power by users and other stakeholders.[15]

13 Jack M. Balkin, "Information Fiduciaries and the First Amendment", UC Davis Law Review, Vol. 49, No.4, 2016, accessible at https://lawreview.law.ucdavis.edu/issues/49/4/Lecture/49-4_Balkin.pdf.

14 Richard S. Whitt, "Old School Goes Online: Exploring fiduciary obligations of loyalty and care in the digital platforms era", Santa Clara High Technology Law Journal, 2020, accessible at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3427479.

15 Sean McDonald, "The Fiduciary Supply Chain", Centre for International Governance Innovation, 2019, accessible at https://www.cigionline.org/articles/fiduciary-supply-chain.

The critique of the information fiduciary approach[16] is chiefly that it fundamentally ignores that the schism between the interests of users and data processors persists despite the fiduciary framework. Expecting information fiduciaries to independently act in the interest of users is moot when the premise of their business models is opposed to giving users control to prevent third party data sharing. Futher, the fiduciary framework lacks the infrastructure to be effective in operating against entrenched business models, and by attaching notional responsibility to data processors, it negates the possibility of regulating their business practices, which occupies the core of the conflict to user rights and interests.

16 David E. Pozen & Lina M. Khan, "A Skeptical View of Information Fiduciaries", Harvard Law Review, 2019, accessible at https://harvardlawreview.org/2019/12/a-skeptical-view-of-information-fiduciaries/.

VII Data Trusts in India

Trust law in India is based on the Indian Trusts Act of 1882 and the attendant judicial pronouncements. While the concept of Trust law has been taken from the English legal system, it has had a parallel evolution in India as opposed to the UK. A trust in Indian law is a trust a set of obligations attached to the ownership of a property, where the obligations of the owner ('trustee') are towards the benefit of a specific person ('beneficiary').

The legal duties associated with Trust law in India are chiefly with regard to maintenance of the property, transparency of accounts, and usage of the property in the interest of the beneficiary. Legal structures around Trust law have remained specific to the nature of property management and discharging of duties[17] in relation to ownership of property and duty of care towards beneficiaries. The principle of a duty of care has been put forward in Indian law in the Personal Data Protection Bill, with a number of requirements in the interest of the user in Chapter III, along with Penalties for violation of these requirements specified under Chapter VI of the Bill.

Data Trusts in India: the Report by the Committee of Experts on Non-Personal Data

The use of data trusts in India has emerged significantly as part of the draft report released by the Committee of Experts on Non-Personal Data. 'Data Trusts' have in the Report been presented as elements of "data infrastructure", a term left undefined in the policy. Data Trusts here are little more than a tool for 'Data Trustees' and 'Data Custodians' to manage the data over which they exercise control. Both these bodies are part of the larger framework of the draft policy—'Data Trustees' represent the interests of user groups (referred to in the draft as Data Principal groups/ communities) and communicate them to other stakeholders, while 'Data Custodians' are data fiduciaries that are reposed with a duty of care by the policy, in favour of the aforemention Data Principal Communities.

17 Apart from management of religious institutions, which is seen as a charitable purpose without a specific beneficiary.

The Report does not go into the specifics of the nature of Data Trusts in this context, beyond a mention of them as an "institutional form of data infrastructure", used to control data sharing and usage. Nonetheless it does ascribe a few functions to the Data Trust, such as anonymisation of the data and providing a common platform for pooling of data by a variety of organisations. It is also mentioned that the Data Trust may be geared for public use. Separately, the policy also states that Data Trusts may also serve as a vehicle for mandatory data sharing sought by the Government—and that in this case such a Data Trust may be managed by a public authority, or neutral bodies such as cooperatives or industry associations.

A significant oversight in the policy is regarding enforcement of the fiduciary duty created by the policy for Data Custodians. The policy does state that Data Trustees communicate the interests of users to Data Custodians—but does not mention what tools may be available to use in the enforcement of these interests. In other words, there is no effective accountability process included as part of the structure offered by the policy. For example, it is not clear what mode of action is available to a Data Trustee may take in case of a breach of duty of care by a Data Custodian. Similarly, it is also unclear how Data Principal communities may negotiate the articulation of their interests by the Data Trustees—the policy has omitted to consider a situation of an objectionable representation of Data Principals' interests by Data Trustees.

As explained earlier, introduction of a seeming fiduciary body does not serve the purpose sufficiently unless there are complementing accountability structures around these bodies. The accountability and representation measures are what serve to create trust in the system from stakeholders. This includes not only users, but also third parties who see themselves as vendors and providers of data and service providers who utilise data for value-added services. Without demonstrable effectiveness of channels of communication and responsive regulatory measures, the proposals are likely to experience a prolonged period of failure due to lack of cooperation from the ecosystem.

VIII Data Trusts in the UK & EU

In 2019, the Open Data Institute[18] a research organization in the UK which does research around the subject of data stewardship, contracted a team of experts to look into the question of whether Trust law can be applicable for the purpose of enabling responsible data sharing.

The report helps move the discussion from using Trust law for data stewardship from the conceptual theory to legal principles. To do this, the report discusses potential forms a data trust may take. Firstly, on the form of a traditional legal trust, the structure involves the creation of a legal entity to whom property is transferred according to certain duties with respect to usage of the property, in this case data. The draws of this approach include enforcing fiduciary duties on the data trust and holding the trustees liable through established existing trust law, which in the UK has plenty of precedent for application.

The problem presented here however, is that data is not transferable property in a majority of legal regimes, including in the UK. Therefore, structuring duties of a data trust would not be feasible under the construct of a legal trust. This approach also restricts holders of data from forming a data trust because Trust law prohibits trustees from benefiting from the property themselves.

An alternative approach to structuring a data trust is through a set of agreements defining the roles and responsibilities of the parties to the arrangement. The data trust here would be permitted to process data as per terms of the agreement, and further share data to third parties with similar restrictions.[19] However, without an existing legal regime ensuring the discharge of these functions, the arrangement would amount to a the same form as a bilateral data sharing agreement, without participation from users or any specified 'beneficiaries'.[20]

18 "ODI report: Data trusts: lessons from three pilots", Open Data Institute, 2019, accessible at https://docs.google.com/document/d/118RqyUAWP3WIyyCO4iLUT3oOobnYJGibEhspr2v87jg/edit?usp=sharing.

19 "Extended ODI Data Trust report: further use cases to consider", BPE Solicitors, accessible at http://theodi.org/wp-content/uploads/2019/04/BPE_PITCH_EXTENDED_ODI-FINAL.pdf.

20 Jack Hardinges, "Data Trusts in 2020", Open Data Institute, 2020, accessible at https://theodi.org/article/data-trusts-in-2020/.

The TRUSTS Project in the EU

The EU is in the process of initializing a project to create a data sharing marketplace, called the TRUSTS project.[21] The project falls under the larger objective to create a platform where data providers can create a common pool of shared data that can be used by participating companies for analytics and derived profit, but also for public benefit by municipal authorities and civil society.[22]

This follows the recommendation from the European Commission in its Data Strategy document[23] on the creation of a common regional platform for data sharing in specific sectors. These platforms seek to enable deployment of data-sharing tools and platforms, creation of data governance frameworks, and improve the availability, quality and interoperability of data. The plan involves creation of standards that apply across sectors, but also tailored measures that remain in domain-specific settings.

An additional piece of context is the ongoing work of the High Level Expert Group on Business to Government Data Sharing.[24] The Expert Group has been appointed by the Commission to expedite collaborations in private sector data sharing to create incentives and structures for increased collaboaration and data sharing for public purposes.[25]

21 Accessible at https://www.trusts-data.eu/.

22 "A Digital Single Market Strategy for Europe", European Commission, 2015, accessible at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN.

23 "A European Strategy for Data", European Commission, 2020, accessible at https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf.

24 "Meetings of the Expert Group on Business-to-Government Data Sharing", European Commission, accessible at, https://ec.europa.eu/digital-single-market/en/news/meetings-expert-group-business-government-data-sharing/.

25 "Analytical Report 12: Business-to-Government Data Sharing", 2020, European Data Portal, accessible at https://www.europeandataportal.eu/sites/default/files/analytical_report_12_business_government_data_sharing.pdf

IX Conclusion

In the discussion above, we have seen that the legal regimes operating within the common law context of India and the UK are not equipped with tools of investing data sharing with fiduciary responsibility for a number of reasons. Significantly, data is not a form of property whose ownership in clear and transferable, and therefore cannot be invested into a classical legal trust with attendant fiduciary responsibilities.

Legal regimes which have instituted an operative form of the concept of data fiduciaries also stray from the idea of fiduciary responsibility insofar as they do not require these data fiduciaries to act on the interest of users—the laws in fact place restrictions and penalties on these fiduciaries, against the possibility of violation of consent and processing of user data against the interests of users. The valid assumption made by these laws of data fiduciaries acting in their own interest, and not those of the users, indicates that the legal and economic structures around them are not designed for them to serve users and prevent misuse of data.

Policy experiments around using Trusts for data sharing are still missing the component that allows enforcement of fiduciary responsibility. While common law has a solid understanding of enforceability of fiduciary responsibility under Trust law, this mainly applies to directions and corrections in usage of property. Data, not fitting this regulatory format, is less suitable to the Trust framework. This is made clear in the existing efforts to bring in an operation form of it in India and the UK—reports on these efforts make clearer the problem of a lack of accountability of these Trusts to their beneficiaries—be it individual users, or larger communities.

What is needed is a tool to operationalise enforcement of users' rights and interests against third parties. Users need to be able to interact with the entity that handles data sharing—be it a data fiduciary or a data trust—and influence how their data is used. This requires a mode of participation and representation from users. Legal and policy fictions of Trusts and other intermediaries may only work as long as they provide a clear path towards articulation of user preferences, and avoid the continued centralisation of decision-making.