Understanding Data Trusts

The GPAI Data Governance Working Group
July 2021

Understanding Data Trusts

At this year's summit, G7 leaders reiterated their commitment to promoting a human-centric approach to Artificial Intelligence (AI) and to supporting forms of data governance that enable the widespread use of data for public benefit. Identifying and understanding the data stewardship approaches that can support human-centric AI are central to GPAI's data governance work. GPAI's members are brought together by a shared commitment to the values set out in the OECD Recommendation on Artificial Intelligence, and to the development of AI that is rooted in the principles of human rights, inclusion, diversity, innovation, and economic growth.

Progress in AI requires access to data, and data stewardship offers an important lever in shaping how AI technologies develop. Who shares data, for what purpose, and for whose benefit are central to the development of trustworthy AI technologies. With these questions in mind, our new project, *Enabling data sharing for social benefit through data trusts*, is investigating how new forms of data stewardship can enable access to data for innovation while putting citizen interests at the heart of data stewardship.

Different approaches to data stewardship already exist, supported by a variety of data institutions that help different users access data under controlled conditions. The term 'data institution' is generally used to refer to an established structure that stewards data on behalf of a community. These fulfil different functions: some might act as an intermediary organisation offering data management services; some might pool data for common use; others might take the form of an 'escrow' service that manages how different parties interact with data resources.

Data institutions can take different forms. In some cases, they might be a set of technologies that govern how data can be accessed or processed. In others, they could be a set of legal agreements and organisational practices that determine how decisions about data use are made. In some cases, institutions might have a formal legal basis, being officially incorporated as an organisation, but a variety of other relationships or data sharing regimes might also form the basis of a data institution.

Understanding data trusts

In recent years, data trusts have emerged as a novel approach to data stewardship. Data trusts are a type of data institution that supports individuals or groups to pool resources, tasking an independent 'trustee' to manage those resources for the benefit of the trust's members. While the specific motivations of those setting up a data trust will vary in different contexts, data trusts are characterised by their focus on:
- enabling data-driven innovation for social and economic benefit, by creating a trustworthy environment for data sharing.
- re-balancing power asymmetries in data exchanges, by encouraging and empowering the originators of the data to play an active role in setting the terms of data use – and the distribution of the value that creates – and providing a platform for collective negotiation; and

- anticipating, preventing, and managing the vulnerabilities associated with data use, through professional data stewardship.

One of the distinctive features of a data trust, in contrast to other types of data intermediary, is the concept of 'bottom-up' engagement. Data trusts should offer a vehicle for individuals or groups to choose how they want data that is about them to be used, engaging a trustee to make decisions about data use on their behalf. This relationship implies a set of functions specific to data trusts. Data trusts will need to:
- provide a platform for collectives to establish desirable terms and conditions of data use, setting the constitution of a trust;
- appoint expert trustees (professional managers) to take responsibility for the stewardship of the trust's assets,
- create a regime of strong fiduciary responsibilities to bind the trustees to act in the interests of the trust's members;
- negotiate use of trust assets in accordance with agreed terms and conditions, facilitating safe and controlled data use; and
- establish safeguards and oversight mechanisms to prevent data misuse and to take remedial action in the event of the trust's terms and conditions being breached.

The fiduciary responsibilities created by the trust demand that the trustee acts with undivided loyalty towards the members of the trust – the trustee is legally and ethically required to act in the interests of the trust's beneficiaries. These duties help create an environment of strong institutional safeguards that are particularly important in mitigating the vulnerabilities that can arise from data use – particularly when that data is about people.

Many different types of data can be useful in the development of AI technologies in different contexts. Not all this data is 'personal', relating directly to an individual, but as AI technologies develop the distinctions between personal and non-personal data are becoming blurred. Datasets that might seem uncontroversial can – if combined an analysed in new ways – generate sensitive insights. As a result, our work on data trusts is taking a particular interest in the governance of data about people, and how to steward that data in a way that serves their interests. However, it is also possible to envisage scenarios in which data trusts might be used to serve organisational needs. Where data exists about an entity, data trusts are a way of returning control over how that data is used and what value it helps create to that entity.

Enabling data sharing for social benefit through data trusts

If successful, data trusts could provide a platform to connect citizen interests to the purposes for which data is used, creating new opportunities for data-enabled innovations that serve the public interest. In addition, central to data trusts is open data and how 'openness' as such can foster developments in AI technologies and enable North-South, South-South and triangular collaborations. Understandings of how to design and operate data trusts are in flux. This is a nascent and multidisciplinary area, and more work is needed to investigate how a data trust would work. In practice, it seems likely that any data trust will deploy a range of policy, legal and

technical mechanisms to create secure and trustworthy operational practices, reflecting the environment in which it operates and the purposes for which it was constituted. However, important questions remain about how these different mechanisms serve the core functions of these data trusts.

Adding to this complexity, the nature of the rights that individuals have over data about them, the practices that determine how data is shared, and the ways in which concepts like 'fiduciary duties' are interpreted all vary across countries. Data trusts will need to develop ways of working that serve communities with different issues, concerns, and in areas with different types of institutional capabilities. They may need to operate in environments where both regulatory provision and the ability of courts to directly intervene and adjudicate in cases of data misuse is limited, taking different operational strategies in each case.

There has already been much interest in data trusts at a national level in countries across the world. To make progress, we need to build on these national efforts, learning from each other's experiences and creating new collaborations. GPAI's data trusts project will mobilise the expertise of the international community to improve our understanding of the role data trusts can play in trustworthy data stewardship and of the operational considerations that will influence their ways of working. Over the course of the project, we hope to explore:

- When data trusts are helpful, describing the scenarios, dynamics of the relationships and nature of data (and data sharing) that favour the use of data trusts over other governance interventions.
- How data trusts can help resolve the tensions that emerge in data use – between individual and group interests, and between the desire to promote data use for innovation and the need to protect citizen rights (whether set out in legislation or relating to wider human rights).
- How to design and run data trusts, looking at which combinations of technical, legal and policy mechanisms can help create a trustworthy stewardship environment, what types of interactions between individuals and data trusts will provide positive user experiences, and how trusts can be made financially sustainable over the long-term.
- How data trusts can be made accessible and responsive to community needs or interests, especially when there may be conflicts of interest between different parties engaging with a trust.
- What legal interventions can support the collectivisation of rights, and help individuals exercise their data rights. In common law countries, for example, trust law could provide a framework for data trusts, creating a regime in which trustees owe fiduciary duties to the beneficiaries of the trust. Other frameworks will also allow for the creation of professional trustee managers, responsible for the administration of a data trust.

Our first outputs will be published later this year, which we hope will start a conversation with the wider community about what action is needed to make data trusts accessible and beneficial to all in society.