Data Trusts

Note of a workshop sponsored by The Alan Turing Institute and Jesus College Intellectual Forum

23 September 2019, Jesus College Cambridge
Co-organised by Sylvie Delacroix, Julian Huppert and Neil Lawrence, with support from Jessica Montgomery

---

In September 2019 The Alan Turing Institute and Jesus College Intellectual Forum co-convened a workshop to explore the potential of Trust law as a framework for enabling careful stewardship of data use. This note summarises discussions at the workshop. It is not intended as a verbatim record, and does not reflect an agreed position by workshop participants.

Background

The problem: Shifting patterns of data generation and use are creating new kinds of vulnerabilities, as well as potential harms to individuals and society. Different approaches to the governance of data have been proposed, but many of these rely on core concepts (such as ownership, or consent) that are creaking under the pressure of digital change. They also often rely on individuals investing resources in asserting their rights through complex legal processes. At the same time, public dialogues on data consistently show people have a desire for more agency in decisions about data management and use. There is a growing awareness of the need to empower groups, not just individuals, given the power concomitant with aggregated data. Alternative governance approaches are needed that allow individuals to work collectively, defining desirable terms of use and harnessing the use of data for public benefit.

The proposal: Trust law provides an apt legal framework to manage the vulnerabilities created by changing patterns of data use. Aside from the fiduciary responsibilities imposed on trustees, Trust law also provides unique legal oversight mechanisms that can address current power asymmetries in data use.

The rationale: While existing frameworks have enabled data sharing between organisations in defined circumstances, further action is needed to create an environment in which individuals or groups are able to influence how data about them is used, and for what purpose. Trust law is flexible enough to allow for the variety of different potential uses of data and to take into account the new capabilities that might arise from technological advancements. It is also well-suited to creating structures that support collective action to assert data rights.

The workshop: In September 2019, participants gathered at Jesus College, Cambridge, to explore how Trust law can contribute to data governance. These discussions built on previous work, notably: Delacroix, S. and Lawrence, N. (2019) Bottom-up data Trusts: disturbing the 'one size fits all' approach to data governance , *International Data Privacy Law,* ipz014, https://doi.org/10.1093/idpl/ipz014

Discussion summary

A shifting data environment

New forms of harm require new governance systems

Interactions in the workplace, at home or with public services are increasingly data-enabled, mediated by digital technologies that promise to boost economic growth and enhance societal wellbeing. In pursuing these everyday activities in the digital environment, individuals leave a trail of data. There are already instances of seemingly innocuous data about individuals being linked in ways that generate sensitive insights, or of behavioural information about individuals being used to shape significant social and political debates, with implications for both individuals and society.

These potential harms demand fresh approaches to data governance, based on visions for the future in which individuals can play an active role in shaping how, when, and why their data is used (and by whom). Current approaches to data governance, however, grant relatively limited influence to individuals, or rely on citizens pursuing their individual rights through time- and energy-intensive legal processes. Alternative approaches seem better suited to the challenge of democratising the digital revolution, and Trust law's combining of robust safeguards with adaptability to social change makes it a well-suited framework to achieve this goal.

Frameworks for enabling data use: the role of Trusts and other legal mechanisms

A range of legal mechanisms to support data use exist, including access arrangements that support organisations to combine and analyse their data for public benefit. For example, a recent project explored the use of data sharing agreements to create new tools to tackle the illegal wildlife trade, combining datasets from different organisations to allow novel analysis and use. In such cases, where data does not give rise to personal or intellectual property rights, effective data management may be best achieved through 'horizontal' (or inter-organisational) agreements or a data commons framework, with appropriate access accreditation mechanisms. These arrangements need not necessarily rely on Trust law, and do not tend to make provisions for managing vulnerabilities or the collective assertion of data rights.

The term 'Data Trust' has proliferated in recent years. Trusts, however, have characteristics that allow them to play a specific role in stewarding data use, alongside particular requirements for their establishment. A Trust is formed when a person in whom a set of resources is vested – the Trustee – is compelled to hold and manage those resources either for the benefit of another person, or for some legally enforceable purpose. Creating a legally-effective Trust requires a subject matter (which need not be defined as 'property'), identified beneficiaries (or an exclusively charitable purpose), and a trustee to hold the Trust's assets. Trusts must also have time limits; they cannot operate in perpetuity. Core to the operation of Trusts are the fiduciary responsibilities they impose on Trustees: a Trustee is bound by this responsibility to the data subject, being required to act with impartiality, prudence, transparency, and undivided loyalty. It is this responsibility, and the oversight mechanisms that ensure that Trustees carry out this responsibility, that uniquely positions Trust law to address the current power asymmetries in data use.

The term 'data trust' has proliferated in recent years

Widespread use of the term 'trust' to refer to a variety of data sharing arrangements could risk diluting the power of this proposed approach. As debates about how best to develop trustworthy data governance mechanisms develop, care is required to avoid so-called trust-washing exercises, in which the terminology of data trusts is applied to systems that do not enable meaningful public engagement or support the collective assertion of data rights

The demand for data Trusts: Inertia, vulnerability, and opting in

To be effective, Trusts must be accessible to a wide range of people. Not feeling empowered or informed about how Trusts work could create barriers to engaging with their development, which risks perpetuating existing power imbalances: those who have knowledge will be protected by joining, while others may be excluded because they lack that capacity.

This raises questions for the development of data Trusts:

• What would encourage (groups of) individuals to engage with data Trusts?

• How does one avoid empowering only the least vulnerable part of the population?

• Would data Trusts' protective aims be defeated if data subjects were to sign up for more than one?

There are both risks and merits inherent in a 'default opt-in' approach to promoting engagement with data Trusts. The NHS, for example, already uses a 'default' arrangement in some of its digitisation projects, and provides individual protections accordingly. What lessons come from this for data Trusts?

Trusts must be accessible to a wide range of people

Policy and technology infrastructures to enable data Trusts

Trustworthy data governance infrastructures can draw from a variety of different policy approaches, including 'hard' law or regulation; codes of conduct, ethical frameworks or standards; and technical measures that set the bounds of what is possible or that enable certain types of action. In considering the form of a potential data Trust, this latter category plays a particular role in managing the risks associated with different approaches to data use.

Data aggregation can be valuable in enabling some forms of analysis. However, such aggregation also creates risks: that analysis of the aggregated dataset might enable re-identification of individuals, for example, or an aggregated data store might attract higher levels of security threats. In some circumstances, therefore, a data Trust may deem a decentralised approach more desirable.

Trusts will need to negotiate questions about how to manage the benefits and risks of these different approaches, such as:

• Who decides whether to decentralise or centralise data management, and how?

• What mechanisms are required to move data into Trusts, and how would these be administered?

• To whom and for what purposes is an individual authorising data use, how is this reflected in the underlying infrastructure of the Trust, and how can an individual revoke such access?

• What technology infrastructure is needed to support data portability between Trusts?

Cross-Jurisdictional Aspects

Technology markets are global, and data Trusts could play a useful role internationally, providing a local foothold for governance systems that co-exist alongside larger-scale supranational policy mechanisms. For such a system to operate effectively, Trusts will need to find ways of aligning different political systems or cultural factors that influence attitudes to data use. This could require new forms of regulatory oversight in different locations, with the details of regulatory enforcement varying from nation to nation.

Trusts could play a role internationally