Data Trusts – Increasing access to data while retaining trust?

Machine learning relies on having large sets of training data. Generally speaking the more data, the better the results. As AI and machine learning become more widely used, parties benefit from sharing data and need to overcome legal and technical hurdles in order to do so. Companies and organizations who are rich in data can usefully consider data trusts as a way of making data available to others in a safe and trusted manner. AI stakeholders who are seeking data for machine learning can look to data trusts as a source of data. We explain what data trusts are, how they may be used, and what to consider before using a data trust.

Reputational risk

The amount of scrutiny that users and collectors of data are subject to is increasing. In particular, there is a growing demand to reduce the abuse of data, enhance accountability and improve ethical standards, while ensuring that maximum benefits are derived from the use of data. The reputational risk associated with collection and/or use of data is significant and clients are looking for ways to mitigate that risk.

The UK government's independent review of **Artificial Intelligence in 2017** recommended that data trusts should be used as a way to "share data in a fair, safe and equitable way". It also appears that organisations in both the public and private sectors are interested in using data trusts as a way to increase sharing of data whilst ensuring trust is retained. Examples include Ordnance Survey and Transport for London, both of which are organizations with large amounts of data. Hospitals and NHS Trusts are other obvious sources of data.

Legal, ethical and secure

Currently, the term "data trust" is not well-defined and there are many structures which would fall under the term. It is agreed that a data trust should facilitate data sharing between organisations holding data and organisations looking to use data to develop AI, whilst respecting any legal interests in the data such as IP rights. A data trust must also ensure that data is used ethically and that data is held safely and securely and dealt with appropriately if the data trust comes to an end. A data trust has trustees who are responsible for deciding when and with whom to share data, as well as what data is shared and whether such sharing will be to the benefit of the public and organisations using the data. It is envisaged that the creation of data trusts will allow the public to have greater access to and control over the use of their data, which in turn will increase public trust in data-collecting and holding organisations.

Legal structures and technological solutions

There are several alternative legal structures that may be employed for a data trust. As the name suggests, a data trust could be in the form of a legal trust, although some consider that this would be unsuitable, because data is not property in the legal sense and thus cannot form the basis of a trust. Recently it has been suggested that a data trust could be in the form of a legal trust if it holds data rights rather than data itself. Some envisage contractual frameworks (similar to standard data sharing agreements) or suggest separate companies or partnerships set up to manage and provide access to the data. Each structure comes with its own legal issues. Technological controls may be used to bypass such legal issues, but at present no technology exists which can ensure proper data management within the requirements of a data trust.

The term "data trust" is therefore very broad and a variety of types of data trusts are expected to form. End users of data trusts will be from different industries and sectors, and the data trust structures will reflect these differing needs. Any new regulations or technological solutions will need to reflect this need for flexibility.

Public and private sector potential

The Open Data Institute (ODI) recently announced three **pilot studies** to research data trusts. These studies were funded by the UK government and focused on the use of data trusts to prevent illegal wildlife trade, to reduce food waste, and to improve public services in Greenwich.

The ODI found that there is huge demand for data trusts from organisations around the world, and that data trusts could be a useful solution to data sharing where there are conflicting interests between parties. They also suggested that there may be circumstances where governmental or philanthropic organisations should mandate or fund data trusts for specific purposes, such as work on climate change.

The UK government also appears to be investigating potential uses of the huge amount of data held by the NHS. In a recent speech, Secretary of State for Health and Social Care Matt Hancock described the power of genomics plus AI to use the NHS's data to save lives as "literally greater than anywhere else on the planet". In a **report** from May 2018, the House of Commons' Science and Technology Committee also noted that the government could do more to "realise some of the great value" tied up in restricted public data sets, such as those held by the NHS, and hold them in data trusts. It also suggested negotiating for improved public service delivery from developers in return for access to the data, rather than accepting developer's offers.

In addition, the **Centre for Data Ethics** is understood to be working on data trusts in commercial settings that potentially involve personal data. Future pilot studies have also been recommended to explore the application of data trust models to particular use cases.

Compliance considerations

Before setting up or using a data trust, several issues must be carefully considered. Particularly whilst there are no legal structures around data trusts, the following points should at least be discussed to ensure that an organisation is not in breach of any laws.

— **Data protection and privacy** – Unless data sharing via a data trust is disclosed as a purpose and consented to when collecting personal data, there will need to be consent from the data subjects or some other legal justification before sharing. Data trusts themselves will also need to comply with data protection laws. Anonymising data is frequently inadequate to ensure compliance. Furthermore, certain data types (such as DNA sequences) are inherently incapable of being anonymised.

— **Commercial confidentiality** – It may be necessary to take steps to protect commercial confidentiality in data trusts. This is particularly true if, for example, sales data, financial data, or customer data is being shared. Breach of confidence actions require that information is imparted "with the necessary quality of confidence" – this may not be the case in a data trust.

— **Intellectual property rights** – Certain IP rights could exist in the data itself such as copyright or database rights. In this situation, the data trust will need to secure appropriate licences from rights holders and ensure licences are complied with.

— **Contractual obligations** – Before sharing data, data providers will need to ensure contractual provisions do not preclude sharing of data.

Conclusion

Data trusts are likely to become widely used in future. They have the capability to facilitate data sharing, giving organisations increased access to large data sets, whilst retaining public trust by ensuring proper safeguarding of data and providing public benefits in return for such data sharing. The structures of the trusts may vary considerably and several legal issues may surround such structures. In future, certain provisions and regulations may make setting up or using data trusts easier and simpler. In addition, technological advances may allow the legal issues surrounding data sharing to be bypassed, facilitating the creation of data trusts.

In light of these benefits, it seems highly likely that data trusts will become more prevalent and widespread. Such large data sets will enable better AI development, pushing forward the advancement of machine learning and artificial intelligence.

Contacts

Dr Rachel Free
Partner
T +44 20 7067 3286
E rachel.free@cms-cmno.com

Ella Wells
Trainee Patent Attorne
T +44 20 7367 2145
E ella.wells@cms-cmno.com

Further information, including a list of our offices, can be found at **cms.law**