Innovate Cities.

Innovation Writing Series

The Value of Sovereign Data Governance and Social Technology

The Value of Sovereign Data Governance and Social Technology

Written by Jacob Danto-Clancy
Student | Master of Public Policy Program
Social Science, McMaster University

Data sovereignty is generally defined as the authority of individuals to have control over their own data and information. Individual data sovereignty precedes and reinforces other operational data rights like the right to access, to portability, to opt-out and the right-to-be-forgotten (erasure). That said, data sovereignty and supporting policies alone cannot guarantee the diffusion of these rights into the lives of individuals and groups alike. Especially in terms of equity seeking and marginalized groups, certain technologies and platforms are needed on the application side of these policies, like data trusts, to formally operationalize data sovereignty and the rights it implies.

Data sovereignty implies both privacy and utility equally, even though it is commonly assumed that to have a sufficient amount of one, the other has to be compromised. This is likely because there are hardly any viable, already existing options for people to control and govern the data they produce as a by-product of their immediate online engagement with private-sector applications and platforms. As a disinterested intermediary authority, data trusts break this otherwise asymmetrical flow of data and value-sharing between producer and consumer. Like an "honest broker," a trust is able to collect data and allocate access to it in accordance with robust public governance models that prioritize the data sovereignty rights and interests of their beneficiaries, over those of data consumers.

A useful example of a data-trust-as-broker is Finland's **myData**, which is a human-centric, intermediary platform and personal data management infrastructure. People are meant to use **myData** to gain control over their own personal data by downloading it to their devices and transmitting it to other services. Although not labeled a "trust," **myData** acts as a "personal operator" linking individuals, data sources (collectors) and data-using services, letting the individual decide just how and with whom their personal data are shared. **myData**'s mediation of the data lifecycle affords a core interoperability that allows the individual to participate in the data economy with fewer proprietary lock-ins, reduced switching costs, and localized end-device data control inline with the GDPR.[1] Similarly, the data co-op **polypoly** lets users store and share their data on and from their own device through privacy protecting algorithms of the **polyPod** app. The co-op's technology is designed in such a way that their algorithms 'come to the data and not vice versa' to give the user full control over data sharing.

[1] Open Smart Cities Guide V1.0.

In Japan, public/private sector partners are piloting "**personal data trust banks**" that will let individuals derive financial value from controlling their own data. Users can deposit their data with the bank and receive monetary benefit for however they choose it will securely share their data with other third parties. A common use case includes users receiving subscription discounts from ICT providers by authorizing third party access to their viewing histories and interests for the purpose of creating targeted advertising.

Data trusts frameworks can also serve as a means for reinforcing the data sovereignty rights of distinct groups of individuals and collectives. Te Mana Raraunga, or the "Māori Data Sovereignty Network," (MDSN) is one such example. The group advocates for Māori data rights and interests and, like **Canada's Digital Charter**, was designed according to parameters set by The United Nations Declaration on the Rights of Indigenous Peoples (UNDRIP) for the collection, ownership, and applications of the data of global First Nations people. Similar to First Nations in Canada, data about New Zealand's Māori population has in the past been requested, collected, and used without their consent and without beneficial returns. According to MDSN, Māori people are often denied access to data they provide or that is collected about them, and is used in ways that do not meet their needs.[2]

The MDSN asserts two fundamentally different definitions of data sovereignty. **Colonial data sovereignty** typically refers to the idea that data is subject to the laws of the ***nation within which it is stored***. Alternatively, **Indigenous data sovereignty** defines data as subject to the laws of the ***nation from which it is collected***. Māori Data Sovereignty formally recognizes that Māori data should be subject to Māori governance. The Māori's commitment to Indigenous data sovereignty offers a strong argument for how data trusts build capacity and help establish distinct, actionable, and up-to-date sovereignties prepared to control data that necessarily originates from and accounts for cultural and historical uniqueness.

A similar argument for the data governance frameworks of a data trust could be made for the First Nations and Indigenous people of Canada. More precisely, a trust's fiduciary duties could be leveraged by Indigenous and First Nations to enact their data rights. Although Indigenous scholars Tahu Kukutai and John Taylor acknowledge that centralized data collection and storage about Indigenous people is sometimes appropriate, they counter that Indigenous rights always prioritize their people's "right to identity and meaningful participation in decisions affecting the collection, dissemination and stewardship of all data that are collected about them."[3] A trust framework that incorporated the CARE Principles for Indigenous Data Governance could be leveraged by industry leading organizations like the First Nations Technology Council and the First Nations Information Governance Centre to facilitate data-based decision-making and value creation processes in accordance with Indigenous values and interests.

[2] New Zealand Data Futures Forum. 2014. Harnessing the economic and social power of data. https://www.nzdatafutures.org.nz/sites/default/files/NZDFF_harness-the-power.pdf.

[3] Ibid., 5.

On a municipal scale, data trusts can provide a way for citizens to exert "**community consent**" to decide how data about them is collected, stored, and used. More specifically, Sean McDonald of CIGI describes a **civic data trust** – which is in title and intent what Sidewalk Labs attempted with their Urban Data Trust before it had lost Toronto's public trust – as an intermediate fiduciary power that works on behalf of a given municipality to aggregate disparate individual data into **public data** as a shared resource, which unifies public/private opportunities and risks to improve public goods and to pursue the public's interest.

Although most existing data trusts use centralized storage systems, future implementation should prioritize decentralized data infrastructures for the sake of making data sovereignty an actionable reality for users. As with **myData** and **polyPod**, when data is stored on the end device in a decentralized data trust framework, participants get the same level of personalization associated with privatized Big Tech platforms, without the fear of surveillance or of private companies selling their data for profit.

Data trusts, especially ones that use decentralized infrastructures, are a social technology as much as they are a governance technology: they safely store open and extensible data so that individuals can control and choose how its use best reflects their preferences and personal values. One way of making this level of self-sovereign data governance a reality would be in the agile adoption of a data trust framework by individuals, groups, and collectives (like municipalities). **Through a data trust, distinct peoples could share their data openly and safely through a trusted intermediary, whose fiduciary duties commit them to the pursuit of their beneficiary's idiosyncratic interests, without them having to build large and expensive data infrastructures.** Finally, a trust model braced by progressive digital governance frameworks like the GDPR and Canada's Digital Charter guarantees data sovereignty for a diverse set of actors, without violating their privacy and data protection rights.