# 4.8 Data Sovereignty

**More governments see control of national data as a means to protect citizens' rights, develop the economy, and maintain a sense of cultural identity.**

### Context

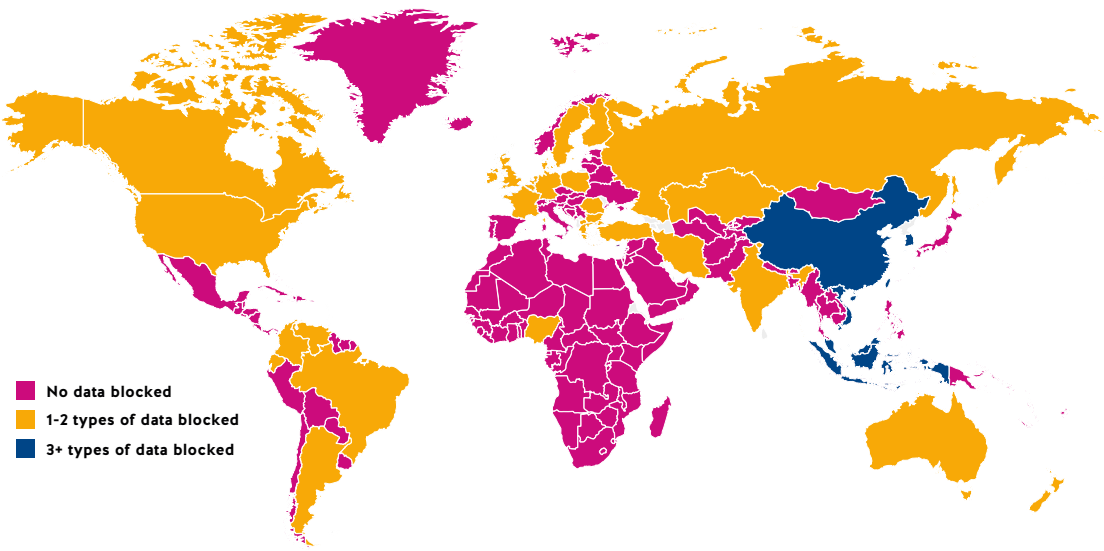
During the early days of the Internet, data flowed freely across national borders by default. The technology made it quick, easy, and cheap, and there were no rules, regulations, or public concern to stop it. Global corporations benefited particularly from this. But there is now a growing push-back.

A rise in nationalist sentiment, mounting fears around privacy and data security, a determination by some to rein in 'surveillance capitalism', and demands that individuals and local economies should get a fairer share of the benefits of data, are all contributing to a worldwide trend to restrict or halt cross-border data flows. Today, over 60 countries are implementing policies designed to do this. Active discussions are underway between national and regional governments and the private sector to shape data sovereignty regulation across the Americas, Europe, and Asia Pacific.[125] Countries as diverse as Russia, Germany, France, Indonesia, and Vietnam have now mandated that their citizens' data is to be stored on physical servers within the country's physical borders; in the US, certain federal agencies require their data be stored exclusively within their national boundaries; Australia has a clearly defined legal framework for health data; Europe's General Data Protection Regulation (GDPR) also restricts organisations from transferring personal data that originated in Europe to any country without adequate data protection laws.

Those who are opposed to this rising trend argue that open data flows are fundamental to today's digital and physical commerce, and a vital catalyst for innovation. Therefore, the ongoing development of the digital economy and continued productivity growth across the more traditional industries, depend on the ability to transfer data, including consumers' personal data, within and between countries for efficient analysis, processing, and storage. Moreover, the freedom to move personal data without restriction between countries generates positive outcomes, not only for organisations, but for citizens and countries as well. This is particularly relevant in countries with an authoritarian government, or where there are restrictions around freedom of speech.

Why then is there still such support for data sovereignty? During our discussions, three primary reasons for its appeal were identified:

1. National Security
2. Citizen Surveillance
3. Data Imperialism




Countries Blocking the Global Flow of Data (2017)

# What We Heard

### National Security

In India, it was observed that in the future, *"the key players will be the data rich, not the richest - the amount and availability of data, rather than the size of the country, will define multinational treaties and data sovereignty power."* Many we spoke to agreed, and there were numerous discussions about how to protect access to sensitive national data of all types, particularly as advances in data technology has made rapid cross-border data sharing easier. In light of this, both American and Chinese surveillance techniques were a subject of intense debate, and our workshops looked at ways in which nations could enhance digital security by limiting cross border data flows and making investments in cloud computing.[126] A number of governments, including those in Brazil, India, and the European Union, have already sought to do this.[127] Elsewhere, conversations in Singapore, Jakarta, and Hong Kong highlighted the need for nations to retain control of their citizens' data, as a matter of national security. The concern in Jakarta was that currently *"all government, corporate, and personal email is largely dependent on western platforms,"* however, *"regulation is in development to address this."*

In Singapore, where trust in government is high, there were strong views about the importance of data sovereignty to ensure national security, particularly with regard to the sharing of health data: Although *"no-one has yet worked out the extent to which patient data can compromise government security……. our existing laws restrict the sharing of personal data (including health data) beyond the national boundary."*

### Citizen Surveillance

Some argue that increasing state surveillance is necessary for national security, but it can also restrict individual rights. In Pretoria, there was recognition of the need to have a nuanced approach to balancing national security, with freedom to share and access personal data. The question was asked, *"how do we manage the legislation of personal communications in the name of national security – particularly in the fragile non-democratic states of Africa?"* They questioned the value of data sovereignty in countries where there is little or no trust in government, and pointed out that *"if there is an international shut down, there is no way of protesting, other than through the internet – data can be used where law can't go."*

> "The key players will be the data rich, not the richest - the amount and availability of data, rather than the size of the country, will define multinational treaties and data sovereignty power."
>
> Bangalore workshop

In Singapore, it was observed that *"the key question is how to establish the hierarchy of rights between individuals, citizens, corporates, and the government."* In China, maintaining control of all the data produced by its citizens enables the government to produce its social credit rating, and is used as a way for the state to maintain control. Every citizen has been given a score based on historical behaviour, and for those with low marks, this means restrictions on access to services and freedom of travel, with, at the extreme, passports being cancelled. This level of surveillance extends across all aspects of an individual's life - in Shanghai, we heard that *"all Chinese health data has to be on one of three government-backed Chinese companies' servers by 2020."* In another China discussion, we were informed about the rise of Internet hospitals, which are consolidating millions of health records and enabling the mass identification of individuals with specific characteristics of concern.

The Russian government is also demanding greater access to citizens' private data. Indeed, President Putin has recently introduced a law on "digital sovereignty," which in theory, will let the Kremlin censor or cut off the national internet. In practice, this would be difficult to achieve, as Russian internet companies have servers abroad and would need Western co-operation to do it. So far, Facebook and Google have resisted Russian requests to reveal their users' identities. But the pressure is mounting on them to comply.

"The key question is how to establish the hierarchy of rights between individuals, citizens, corporates, and the government"

Singapore workshop

### Data Imperialism

Around the world, we heard concern that multinational companies, predominantly from the US, have built huge empires by treating data as a natural resource that can be extracted and exploited without fair recompense to those who generate it.

In Madrid, the consensus was that *"dominant Western services, built by Western engineers, reflecting Western values, and built on Western data, will increasingly be seen as either imperialist interlopers, irrelevant, or inappropriate in different cultural regions."* Elsewhere, there was widespread pushback against what was seen as Western greed. In conversations in both Nairobi and Johannesburg, the discussions focused on how to ensure that African data is not exploited by international companies as if they were just another natural resource. South Africa, for example, has restricted the sharing of blood samples with US-based companies, like ancestry.com and 23andme, for genetic profiling, because it *"does not want 'cheap' African data to be monetised by others."* In Nairobi, the conversation explored ways to protect African culture. Data sovereignty legislation, they felt, would ensure that *"in the future, we can respect the origins of African cultural data and monetise it ourselves."*[128] They also looked at ways in which to protect African data, by introducing *"appropriate [national] regulation and data transparency to move monetisation forward."* These should have "shared value models and clear reporting frameworks."

In Dakar, there was a call for *"the value of data to be used in the national interest, not only for the benefit of international companies."* Similar views were expressed in Abuja. *"Africa needs clearer policies around data – what is being gathered, why, and by whom."* In Abidjan, there were proposals about greater cooperation between African states: *"as concerns around security continue and the confidence of African developers increases, there is a growing appetite for Ivorians to look after the data that they produce, and become less dependent on Western nations."*

> "Dominant Western services, built by Western engineers, reflecting Western values, and built on Western data, will increasingly be seen as either imperialist interlopers, irrelevant, or inappropriate in different cultural regions."
>
> Madrid workshop

In Johannesburg, where the POPI (Protection of Personal Information) Act regulations came into force in December 2018, it was felt that a regional approach to protect citizens' data should be developed in order to boost the local economy. Students in Pretoria agreed, proposing that *"Africa needs its own servers and its own systems,"* as well as advocating *"'data decolonisation', so that Africa can establish control over the data that is generated within its borders."* Assuming government willingness to invest, they were strong supporters of *"the development of media and regionally specific content, using African data so that it would be more relevant to the local market, which in turn will lead to cheaper services and better products for consumers."*

There was some concern that, in reality, some authoritarian nation states would use demands for 'sovereignty' to enable them to peruse their own totalitarian ends, rather than to protect their citizens from 'foreign' intrusion and exploitation. To limit this risk, it was suggested in Johannesburg, that even if a country imposes data sovereignty legislation, there should be internationally agreed *"data dignity metrics,"* which will allow the monitoring and use of data for the common good, while maintaining the *"dignity of private citizens."* This, they felt, would have the advantage of limiting the potential abuse of power. Failure to achieve clarity around this, they feared, would not only restrict freedom of expression, but border protectionism would *"stifle innovation"* and may well, *"…lead to mistrust in the potential for data to do good, while increasing the risk of large-scale commercial and state corruption."*

The workshop in Sydney was sympathetic to the motivations for data sovereignty: *"you want to be manipulated by your own government – not another one."* However, many agreed that it *"depends on the type of data: Singapore may have tight control of health data, but it is open with commercial data. In Australia, we keep our financial service data sovereign."* Taking the long view, the conclusion was that *"a few mega countries can grow their own independent ecosystems, but most others know they are unable to restrict sharing."*

"It depends on the type of data: Singapore may have tight control of health data, but it is open with commercial data. In Australia, we keep our financial service data sovereign."

Sydney workshop

Elsewhere, although there was recognition that data sovereignty has the potential to have an impact, few in the European or US workshops felt that it would actually happen at scale. In London, which took place after the discussions in Africa, the workshop dismissed the idea of data imperialism as unfounded. Their perspective was that *"data sovereignty is not good, and data flows should be ensured."* Similarly, in a San Francisco discussion, data sovereignty was considered to be an over-reaction; one participant suggested, *"worrying about this is like moving the deckchairs on the Titanic – legislation is 5 years behind what is already happening."* The feeling was that, while other countries may be concerned about data sovereignty, *"in the US we are moving ahead and are more focused on making better use of data."* One comment was that *"it seems as though other countries are using data sovereignty as an excuse for not making progress,"* and *"we have bigger issues to address."*

### Implications for Data Value

How data sovereignty is perceived is dependent on a number of different issues and motivations. It is easier to believe that sovereignty is a "good thing" if citizens trust their government to use it to protect their rights and promote their national interests. However, in countries where trust in government is low, data sovereignty regulation could be used to restrict free speech and contact with the outside world. In which case, many would consider it to be a "bad thing."

Size also matters. China, Russia, and India are "big" countries and, arguably, are in a better position to use data sovereignty to their advantage than 'small' ones. Their combined economic clout is certainly significant. Many established Western technology firms are keen to extend access to these profitable markets, as well as those in Africa, which boasts both a youthful population and a rising middle class, so oppose the idea of data sovereignty. Certainly, if the momentum towards data sovereignty continues, a good proportion of future data that is created, may be excluded from the global economy.

It may be that much can be done to limit the very real concerns we heard around the protection of citizen data. Greater trust, understanding, and collaboration between nations is certainly needed. Without this, we can expect even more states will act to constrain trans-national data flows. If this happens, the reaction to the calls for data sovereignty we heard in London and San Francisco seems like a somewhat short-sighted response to a changing political landscape.

> "Worrying about this is like moving the deckchairs on the Titanic – legislation is 5 years behind what is already happening."
>
> San Francisco workshop

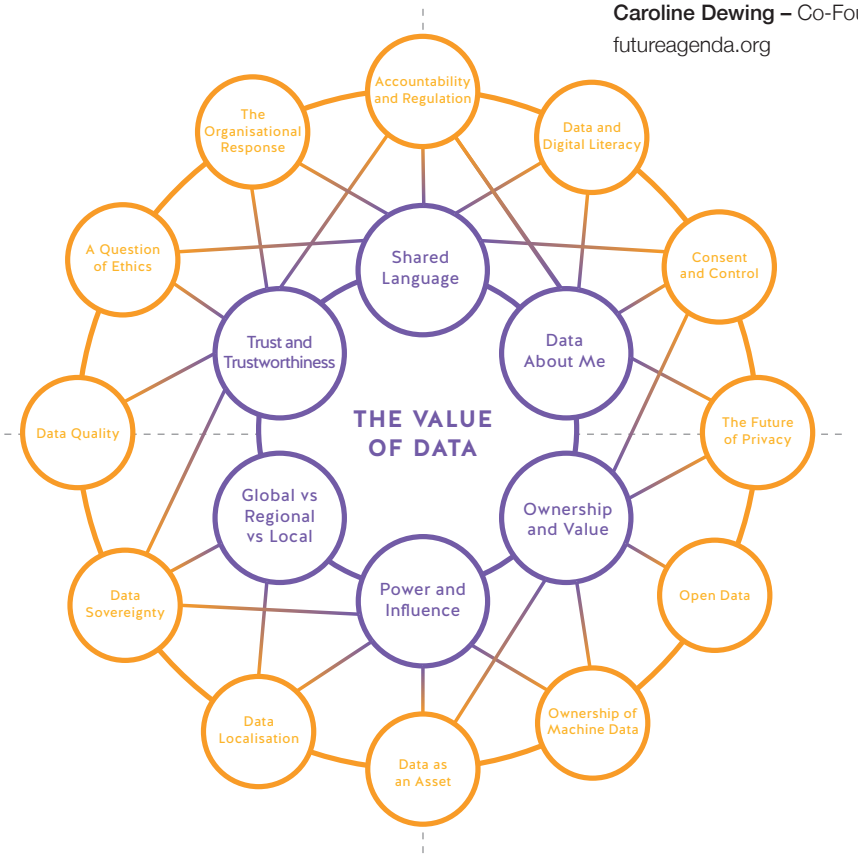
## Context

This is one of 18 key insights to emerge from a major global open foresight project exploring the future value of data.

Throughout 2018, Future Agenda canvassed the views of a wide range of 900 experts with different backgrounds and perspectives from around the world, to provide their insights on the future value of data. Supported by Facebook and many other organisations, we held 30 workshops across 24 countries in Africa, Asia, the Americas, and Europe. In them, we reviewed the data landscape across the globe, as it is now, and how experts think it will evolve over the next five to ten years.

The aim of the project was to gain a better understanding of how perspectives and priorities differ across the world, and to use the diverse voices and viewpoints to help governments, organisations, and individuals to better understand what they need to do to realise data's full potential.

From the multiple discussions 6 over-arching themes were identified alongside 12 additional, related future shifts as summarised in the diagram below.




Details of each of these, a full report and additional supporting information can all be found on the dedicated mini-site: www.deliveringvaluethroughdata.org

## About Future Agenda

Future Agenda is an open source think tank and advisory firm. It runs a global open foresight programme, helping organisations to identify emerging opportunities, and make more informed decisions. Future Agenda also supports leading organisations, large and small, on strategy, growth and innovation.

Founded in 2010, Future Agenda has pioneered an open foresight approach bringing together senior leaders across business, academia, NFP and government to challenge assumptions about the next ten years, build an informed view and establish robust growth strategies focused on major emerging opportunities. We connect the informed and influential to help drive lasting impact.

For more information please see:
**www.futureagenda.org**

For more details of this project contact:
**Dr Tim Jones –** Programme Director, tim.jones@futureagenda.org
**Caroline Dewing –** Co-Founder, caroline.dewing@futureagenda.org


First published November 2019 by:
Future Agenda Limited
84 Brook Street
London
W1K 5EH