Catalyst Cloud
(/)
Sign up (/signup/)

Log in (https://dashboard.cloud.catalyst.net.nz/)

Cloud and sovereignty in Aotearoa

26 August, 2022

What is the cloud?

Cloud computing is today's dominant paradigm in IT infrastructure. It is not new, but is entering the final stages of universal adoption. In a nutshell, the cloud is a natural evolution of IT hosting. Rather than owning and running their own hardware and software platforms, organisations can provision IT services virtually, on-demand, instantly and scalably, on "somebody else's computer", and pay only for what they use.

But cloud is much more than hosting or virtualisation. The internationally recognised NIST Definition of Cloud Computing (/about/news/the-five-essentials-of-being-a-true-cloud-provider/) describes five essential characteristics:

P.

- Multi-tenanting (resource pooling the same physical resources for multiple tenants)
- Self-service, on-demand provisioning. No human involvement needed.
- Wide network access
- Rapid elasticity - scale up and down, illusion of unlimited resources
- Metered usage and billing

The combined effect of these is virtual computing infrastructure that anyone, anywhere, can buy and use "on tap". In some ways, it attempts to turn computing into another utility, like water, or electricity - or the internet.

But, unlike traditional utilities, cloud providers are not required to offer directly compatible services; they can differentiate their products and services as they wish. Depending on who you're talking to, this is known either as innovation, or simple vendor lockin.

Also, unlike utilities, the cloud provider industry is global, not local; you can buy your cloud services from companies on the other side of the world if you want to.

cloud services from companies on the other side of the world if you want to.

The strategic importance of cloud

Worldwide spending on cloud services is expected to reach $1.3 trillion by 2025, reflecting an annual growth rate of nearly 17%. Cloud computing is now the foundation on which everything else is built by default; it is the machinery that runs our government and economy. Cloud computing has gone from experiment to critical global infrastructure in just twenty years. And it has been so successful that we can no longer function as a society without it. Literally.

Our government in Aotearoa has piled into cloud in a big way, shifting identity registers, health and education systems, payrolls, data warehouses, and financial systems, into the cloud.

It's not hard to see why this is happening - the government's Cloud First (https://www.digital.govt.nz/digital-government/programmes-and-projects/cloud-programme/about-the-cloud-programme/) policy requires it, stating "The New Zealand government recognises the benefits of adopting cloud computing as a foundational 'building block' to enable New Zealand's digital economy and digital public service", and "The government's Cloud First policy requires its organisations to adopt public cloud services in preference to traditional IT systems, following risk assessments."

This trend is reflected just as strongly in the private sector, across banking, insurance, agriculture, transport, telecommunications, technology, and media.

The cloud is a revolutionary technological innovation, and one on which we have not just bet the farm; we have bet *all* our farms. In practical terms, there is no area of civic or economic life that doesn't depend on cloud services.

This makes cloud computing a strategic industry of national importance, in the same category as industries such as energy, defence, finance, agriculture and transport.

Building empires in the clouds

So, who owns the cloud?

This is a profoundly important question, because whoever owns the cloud controls the future. If data is the new oil, then cloud providers are the new global oil fields. And, just like oil fields, they give enormous strategic power to the nations that own them.

It's no coincidence that today's top five cloud providers reflect the current geopolitical leaderboard; they are all either American or Chinese. They are Amazon Web Services, Microsoft, Alibaba, Google, and Huawei. Together these five companies control more than 80% of the global cloud provider market. The fight for global economic, political and social domination is being played out in the cloud, where digital empires are real empires, rising and falling.

Perhaps what is most interesting is the geostrategic polarisation in the cloud provider industry. It's dominated by two mutually hostile superpowers. If you're not the USA or China, and you can't (or don't want to) build your own cloud capability, you need to pick sides.

Consequently, the rest of the world has largely split along predictable geopolitical lines. In the EU, for example, Amazon, Microsoft and Google account for 66% of the cloud market, followed by Deutche Telecom in Germany and OVH Cloud in France, with about 2% each.

P.

In Australia and Aotearoa, the picture is even more pronounced, with US cloud providers enjoying near-total dominance.

The global expansion of Big Tech, including the world's biggest cloud providers, is quite literally modern day imperialism. It represents an insatiable quest to gain influence, money and empire.

Internal and external sovereignty

The English word sovereignty has its roots in the medieval Latin "supremitas", then Old French "soveraineté", meaning "supreme power". But it turns out sovereignty isn't just a word we can use without context and expect to be understood. In legal and political theory - and in the history of Aotearoa - the meaning of sovereignty is contested, complex and sometimes contradictory.

Sovereignty can usefully be separated into two related - but opposing - concepts. Internal sovereignty and external sovereignty.

Internal sovereignty describes the power structure within the state, including the power to make or change the law. For example, the internal sovereignty of Aotearoa is embodied by our constitutional monarchy, which describes the power structure between the Sovereign (the head of state), the Governor-General, the Prime Minister, and the executive government conducted by Ministers and their departments.

External sovereignty, on the other hand, is the freedom of the state from external control. It is the independence, autonomy, and self-determination of the state in an international context. While internal sovereignty talks about how the state exercises power within its jurisdiction, external sovereignty talks about how the state is free from any external power being exercised on it. Since there is no agency higher than the state, the starting assumption in international law is the sovereign equality of states.

In reality, of course, an uneven power relationship exists between states, partly in the form of international laws and treaties, but also due to innumerable practical factors that can reduce or undermine a state's independence or autonomy. This is the difference between de jure sovereignty (that which is described by law) and de facto sovereignty (that which exists in reality) - a state may have a high degree of independence under international law, but in practice be subordinate to another nation, or nations.

This last point deserves to be emphasised: internal sovereignty, no matter how good it is, can be totally undermined by a loss of external sovereignty. There's no point just trying to get our internal power structures right - we have to make sure our country has autonomy and self-determination in an international context.

Data sovereignty

Data sovereignty is a special case of external sovereignty, in which data is stored within the exclusive jurisdiction and control of a state.

To establish data sovereignty, data must be held onshore, either by the state itself or by locally owned private companies. This ensures that exclusive jurisdiction is maintained at all times, and that data is free from external control or surveillance.

To be clear, data held onshore by an overseas owned cloud provider is not, and can never be, under the exclusive control of Aotearoa.

The reality is that foreign states can unilaterally assert global jurisdiction over their companies, including subsidiaries in other countries. For example, the United States can exert legal and other pressures on US cloud providers in Aotearoa. This includes the application of laws such as the US CLOUD Act, which can require them to hand over personal data to US authorities, without any authorisation from the courts of Aotearoa.

Another example is Section 702 of the US Foreign Intelligence Surveillance Act (FISA 702), which permits the US government to conduct targeted surveillance of foreign (ie, non-US) persons located outside the US in order to acquire “foreign intelligence information.” Under Section 702, the US Attorney General and Director of National Intelligence may issue directives compelling US electronic communication service providers (ECSPs) to provide such information.

Aotearoa has yet to properly acknowledge or respond to these issues. Indeed, a prevailing view in some government policy circles is that there’s nothing to worry about: first, we can encrypt our data with keys we keep away from US eyes; and second, we will always have legal right to refuse requests to disclose data.

The first point is completely unrealistic on technical grounds, because it would require that customer data is never decrypted or processed in the cloud. You could never do anything with the data in the cloud, because that’s the point of encryption – it’s impenetrable. This is blatantly not what we are doing – instead, we are sending data to the cloud precisely so that it *can* be decrypted and processed, and so that systems and applications can be built that use that data. While data is typically encrypted in transit and while stored at rest, it is always decrypted whenever it is processed inside the cloud.

The second point is simply wishful thinking, without basis in law or practice. The US CLOUD Act allows the US to compel the production of data held abroad. Given US cloud providers have access to our decrypted data, their technicians can access data if compelled by the authorities. Even if we pretend that the courts in Aotearoa had power of veto, it is easy to see the danger of consistently refusing requests of the country that owns the services that power our country. In reality, pressure builds, lines get blurred, and data gets spilled.

European countries are deeply concerned by the security and privacy implications of using US cloud providers. For example, in March 2022, Denmark released its "Guidance on the use of cloud" and dedicates a large section to the topic of "Cloud and the United States". This follows the Schrems II judgement by the European Court of Justice, which found that the EU-US Privacy Shield - one of the primary data transfer mechanisms for the safe and free flow of data between EU and US organizations - is invalid. US laws do not satisfy requirements on data privacy that are essentially equivalent to those required under EU law.

The key point is that laws passed by other countries extend to their companies operating in Aotearoa, and there's nothing we can do about it. Those laws undermine our sovereignty, and materially limit our authority to exercise power within our nation.

In the same way that embassies are extraterritorialities within a country - i.e. they are treated as being the sovereign territory of the embassy's home country - foreign owned clouds operating within Aotearoa are digital extraterritorialities. The data they hold cannot be said to be in Aotearoa, even if the physical servers are. They are data embassies, where the laws of Aotearoa cannot be reliably or exclusively applied.

Māori data sovereignty

The internal sovereignty of Aotearoa is complex and highly problematic, especially given the European colonisation in the 1800s that resulted in He Whakaputanga in 1835, and Te Tiriti o Waitangi in 1840.

Māori did not sign away their sovereignty (https://maorilawreview.co.nz/2014/11/waitangi-tribunal-finds-treaty-of-waitangi-signatories-did-not-cede-sovereignty-in-february-1840/) in Te Tiriti, but rather granted kāwanatanga, or governance, to the Queen of England. From contemporary accounts of hui held in 1840, this was generally understood to mean the establishment of law and order, but many rangatira were deeply suspicious that it ultimately implied subordination. Despite this, most eventually signed.

In return, Māori were promised tino rangatiratanga, or absolute chieftainship, over their lands, settlements and treasures. Lengthy and repeated assurances were made by the Governor and his staff that this was a spiritual and binding contract by the Queen, and that it would be scrupulously upheld. However, in the English version of the Treaty, there is an explicit and total transfer of sovereignty from the Chiefs to the Queen.

Immediately after Te Tiriti was signed, the settler population swelled rapidly, and successive Governors acquired vast areas of Māori land. In 1852, a General Assembly was established to serve the settlers' growing demands for more say over the laws of the land. Only men over 21 with sufficient freehold land could vote, and this effectively excluded Māori. Māori chiefs became increasingly concerned that the rapid and aggressive purchase of their lands was a serious threat to their sovereignty aggressive purchase of their lands was a serious threat to their sovereignty.

The Kīngitanga (Māori King) movement was the direct response to these attempts by the British to assert absolute sovereignty over Māori, and the New Zealand Wars throughout the 1860s resulted in the brutal suppression of Māori and the confiscation of tens of millions of acres of Māori land. This flagrant violation of Te Tiriti, and the unilateral establishment of laws punishing Māori, was a direct and lasting assault on Māori sovereignty, and leaves a bitter legacy to this day.

Māori data sovereignty is principally concerned with redressing fundamental issues of internal sovereignty as it relates to Māori authority over data.

The Waitangi Tribunal has found (Wai-2522 (https://www.bilaterals.org/?waitangi-tribunal-claimants-win-on)) that data is part of mātauranga Māori, and that mātauranga Māori is a taonga. This means that under Te Tiriti, Māori are promised tino rangatiratanga, absolute chieftainship, or sovereignty, over Māori data.

Māori data has very broad scope, and is any data by Māori, about Māori, or about the environments they have relationships with. It is clear that, if and when Māori data sovereignty is recognised and given full effect, it will represent a significant shift in our nation's internal sovereignty.

Māori data sovereignty is not limited to regaining control from the Crown, but is conceived holistically and according to principles of Tikanga Māori. This includes the assertion of external sovereignty, by resisting offshoring of data, and requiring control and jurisdiction over data, including the physical and virtual storage. Māori data sovereignty requires both the internal and external sovereignty of Māori data to be restored.

Operational sovereignty

Operational sovereignty, also called "digital sovereignty", is another special case of external sovereignty, in which the state has full independence and operational control over its digital technology and infrastructure.

Unfortunately, our operational sovereignty is already significantly undermined. Aotearoa is heavily dependent on overseas cloud providers for the day-to-day running of our nation. We depend on their products, features, prices, availability, terms and conditions, all of which are completely outside of our nation's control.

This power relationship is hopelessly one-sided. To the US cloud providers, we are a tiny market, little more than a rounding error on the annual accounts. But to us, the US clouds are all-powerful: without them we won't have an economy or a functioning

public service. Our society and our nation will soon be entirely dependent on these overseas companies. This is the very definition of the loss of sovereignty, the loss of our independence, autonomy and self-determination.

Many people want to believe this isn't a real problem. There's no risk in practice, they say, because we are in the safety of familiar, big brands from an ally we look up to, a values-aligned western democracy, and a superpower. This is dangerously complacent.

Instead, it is safe to assume that US cloud providers would exit the Aotearoa market if became unprofitable or no longer suited them for any reason. It would be naive to expect that a US multinational would nobly sacrifice commercial advantage for a foreign state's benefit. Consider the case of US tech giant Amazon, which in 2021 pulled its $1 billion-plus Lord of the Rings TV show out of Aotearoa (https://www.stuff.co.nz/entertainment/tv-radio/126062311/economic-development-minister-stuart-nash-gutted-to-hear-lord-of-the-rings-production-moving-to-uk), at short notice, and at huge cost to our economy.

What's worse, our government would not be able to prevent such an event. By concentrating our nation's critical systems in a handful of overseas private companies, we are placing those systems beyond our control, and just hoping for the best.

The European Union is tackling the same issue (https://www.weforum.org/agenda/2021/03/europe-digital-sovereignty/). In March 2021, German Chancellor Angela Merkel, Danish Prime Minister Mette Frederiksen, Estonian Prime Minister Kaja Kallas and Finnish Prime Minister Sanna Marin sent a joint letter to European Commission President Ursula von der Leyen. "Now is the time for Europe to be digitally sovereign (https://www.politico.eu/wp-content/uploads/2021/03/01/DE-DK-FI-EE-Letter-to-COM-President-on-Digital-Sovereignty_final.pdf)", they say, by identifying and strengthening systems of critical technologies and strategic sectors.

This is not about withdrawal, or creation of a hermit state: "Digital sovereignty is about building on our strengths and reducing our strategic weaknesses, not about excluding others or taking a protectionist approach. We are part of a global world with global supply chains that we want to develop in the interests of us all. We are committed to supply chains that we want to develop in the interests of us all. We are committed to open markets and to free, fair and rules-based trade. This is what digital sovereignty means to us."

However, the European leaders insist that the EU must actively assert its autonomy and self-determination, explicitly wriggling free of external control: "In order to avoid dependencies, open markets and open supply chains shall be ensured. If this is not possible, then mutual interdependencies shall be established (i.e. no one-sided dependencies on monopolies or countries). As a last resort, European competences and capabilities shall be actively promoted and expanded."

Australia (https://www.governmentnews.com.au/govt-considers-tightening-data-hosting-rules/) has exactly the same threats to its sovereignty, and appears ready to act. Australian government services minister, Stuart Robert, said, “We think there is a case, and we’re exploring this now, for Australian datasets to be in Australian data centers, run by Australians with Australian providers, and securely housed and routed within Australia, to give maximum assurance to Australians that their data’s safe.”

Australia's Whole-of-Government Hosting Strategy (https://www.dta.gov.au/our-projects/hosting-strategy/overview) has adapted to the changing technology landscape. The top two emerging challenges it seeks to address are exactly as discussed above - data sovereignty and operational sovereignty:

- "emerging risks to the sovereignty of data held in Australian Government data centres"
- "increasing risks to the sovereignty and security of the hosting supply chain"

Among global democracies, Aotearoa stands alone, both in downplaying the privacy and data sovereignty risks of using overseas clouds, and in apparently failing to recognise the importance of operational sovereignty and resilience.

Conclusion

Cloud is a strategic national capability, but one that Aotearoa has almost completely failed to build. How did this happen?

The government’s Cloud First policy started with good intentions: government departments should no longer run their IT infrastructure from their basements, but should consume IT as a service from companies that did it better, more securely, and more efficiently.

But there were two unintended and devastating consequences. The first was that it forced IT managers to choose between buying from established US clouds, or investing in companies that were building cloud locally. The lower migration time, cost and financial risk of going with the US providers outweighed most reservations that the privacy or legal teams had, so approvals were obtained and precedent was set. And in so doing, we unintentionally gave away sovereign control of our critical infrastructure and data.

The second unintended consequence was that, because we started buying services from overseas clouds, none of that money was spent on building our own cloud capability in Aotearoa. Everyone knows this is how free markets generally work, but unfortunately cloud was never recognised as a strategic industry worthy of government intervention. Looking back, this was a huge mistake.

As every day passes, we fall further behind in our ability to establish and manage our own critical cloud infrastructure. We have bet the future of our country on an oligopoly of overseas mega-corporations, whose true interests and values can never be said to be those of Aotearoa. By failing to deliberately supplement dominant overseas cloud with locally owned cloud, we have seriously undermined our data sovereignty, Māori data sovereignty, and operational sovereignty.

Aotearoa has a brilliant and innovative technology sector, we have a public procurement purse that can be used to build the future we choose, we have passionate public servants shaping our digital agenda, and we have inspirational Māori leaders who bring a unique, intergenerational approach to thinking and decision making.

It is clear what we must now do as a nation. We must build our own cloud capabilities, repatriate critical data and systems, honour Te Tiriti, and reduce our strategic weaknesses.

A Māori colleague of mine once shared a particularly relevant whakataukī with me: Mā te huruhuru, ka rere te manu – adorn the bird with feathers, that it may fly. For me, this holds special significance in the current context, and symbolises our collective responsibility to make fundamental positive change, and to reach our potential as a nation.

Doug Dixon, CEO

Doug Dixon, CEO

August 2022

Contact us (/contact/)

0800 2282 5683 (tel:080022825683)

Twitter (https://twitter.com/catalyst_cloud)

Linkedin (https://nz.linkedin.com/company/catalyst-cloud-limited)

Careers (https://www.catalyst.net.nz/jobs)

A proud member of

(https://www.catalyst.net.nz/)

Other solutions provided by Catalyst (https://www.catalyst.net.nz/)

Terms & Conditions (/about/terms-and-conditions/)

Feedback (/contact/)