TE KĀHUI RARAUNGA

Māori data sovereignty and offshoring Māori data

CONTENTS

Executive summary

Government agencies in Aotearoa New Zealand (Aotearoa) are increasingly offshoring their data, citing greater security and reduced cost as key factors.

As the government accelerates its digital transformation strategy across the public service, Māori data sovereignty requirements must be central to decision making, particularly with regard to offshoring and procurement.

This requires a more considered, intergenerational approach to data governance and stewardship than the current narrow focus on assessing offshoring risks through a cost benefit lens.

Consideration of a suite of options including strategic investment in locally-hosted solutions would not only give greater effect to Māori data sovereignty, but also enhance the public service drive for digital transformation.

Authors

Tahu Kukutai[1]
Data Iwi Leaders Group technician
Prof, Te Ngira: Institute for Population Research, University of Waikato

Vanessa Clark[1]
Te Kāhui Raraunga Technician and Research Developer (Māori Engagement), Research and Enterprise, University of Waikato

Chris Culnane[2]
Principal, Castellate Consulting Ltd.

Vanessa Teague[3]
CEO, Thinking Cybersecurity Pty Ltd. and A/Prof (Adj.), Australian National University

Introduction

Government agencies in Aotearoa New Zealand (Aotearoa) are increasingly offshoring New Zealanders' data, citing greater security and reduced cost as key factors (New Zealand Government, 2017). Since 2012 the Government has moved at pace to accelerate the adoption of public cloud services as a key pillar of digital transformation (Minister of Internal Affairs, 2016). The Cloud First policy requires agencies to adopt cloud services in preference to traditional IT systems - the rationale being that they are "more cost effective, agile, are generally more secure, and provide greater choice."[4] As a Five Eyes partner, Aotearoa's adoption of a Cloud First policy aligns with the direction taken by partner countries the United States (USA), United Kingdom (UK), Canada, and Australia.

The Government Chief Digital Officer is responsible for setting digital policy and standards which includes cloud services as part of technology and architecture.[5] Adoption of cloud services is on a case-by-case basis with agencies required to undertake risk assessments,[6] including risks relating to jurisdiction.[7] Several pieces of foreign legislation are especially relevant for assessing jurisdictional risk. Australia's Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 makes it mandatory for any organisation whose website or data is hosted in Australia to give authorities access to their IT system if requested (Mann, Daly & Molnar, 2020). [8] The United States Clarifying Lawful Overseas Use of Data Act (CLOUD Act) allows federal law enforcement to compel U.S.-based technology companies to provide requested data stored on their servers, even when the data are stored on foreign (e.g., Aotearoa) soil (Bilgic, 2018). New Zealand Government officials are currently assessing the need for a bilateral agreement with the United States which has already reached agreements with the UK (2019),[9] and Australia (2021).[10]

Furthermore, with Aotearoa's accession to the Budapest Convention,[11] the Government's commitment to co-operation will require changes that include the introduction of data preservation orders, introduction of third-party confidentiality orders, and adjusting mutual assistance laws.

All-of-government (AOG) Cloud Framework agreements are now in place with most of the major multinational cloud service providers including Amazon Web Services (AWS) - which has an Asia Pacific AWS Region in Sydney – as well as Microsoft, SAP, TechnologyOne and Oracle.[12] Aotearoa's sole locally owned and operated cloud provider, Catalyst Cloud, very recently inked an AOG Cloud framework agreement.[13] Alongside these agreements, there is increasingly commitment to build hyperscale data centre infrastructure in Aotearoa. Microsoft has announced that it will build a New Zealand data centre region in Auckland,[14] while data centre start-up Datagrid will build a hyperscale data centre in Invercargill,[15,16] and AWS[17] plans to open an Asia Pacific (Auckland) AWS Region in 2024. In these examples, hyperscale refers to data, compute and storage (at scale), while microscale refers to delivery to the (network) edge.

As the Government accelerates its Cloud First policy, it is crucial to consider how it can both protect Māori data sovereignty and meet its obligations under Te Tiriti o Waitangi. *The Strategy for a Digital Public Service* sets a whole-of-public-service direction for inclusive digital transformation (New Zealand Government, 2020), and has a stated commitment to Tiriti partnership, and to ensuring that Māori are involved in decisions relating to digital transformation of the public service. Taking this commitment as a starting point, this paper considers how government decision-making relating to cloud services and data storage solutions can uphold its Tiriti obligations and meet the requirements of Māori data sovereignty (MDSov hereafter).

This paper makes four high-level recommendations:

1. that Māori, as a Tiriti partner, are involved in policy setting and system-level decisions regarding the digital public service transformation across key public sector agencies;

2. that Māori, as a Tiriti partner, are involved in system-level decisions regarding AOG procurement policies and use of onshore and offshore cloud-based services;

3. that MDSov requirements are developed and incorporated into contractual agreements such as Master Services Agreements (e.g. Cloud Framework Agreements) for the use of onshore and offshore cloud-based services; and

4. that there is strategic investment in a wider range of options to enable both Tiriti partners to give effect to MDSov. Options beyond public cloud (offshore) could include public cloud (onshore), hybrid or multi cloud (onshore/offshore), private or community cloud (Māori-owned, Māori-hosted onshore storage solutions) or fit for purpose agreements with cloud-service providers and non-cloud providers to establish hybrid (Māori federated) Māori 'data islands' within Aotearoa.

To provide context, the next section discusses MDSov concerns and the Government's current approach to offshoring. It then compares cloud-based options involving a mix of locally-owned and foreign hosted solutions before considering ways forward and elaborating on these recommendations.

Indigenous and Māori data sovereignty

Māori data sovereignty refers to the inherent rights and interests that Māori have in relation to the collection, ownership, and application of Māori data, regardless of where it is processed or stored (Te Kāhui Raraunga, n.d.; Te Mana Raraunga, 2018). Māori data has been defined as digital or digitisable information or knowledge that is about or from Māori people, language, culture, resources or environments (Te Mana Raraunga, 2018; see also, Te Kāhui Raraunga, n.d.). In so far as MDSov privileges Māori authority over Māori data, it challenges taken-for-granted assumptions about the nation-state as having sole jurisdictional rights over data (Cormack, Kukutai & Cormack, 2020).

As a collective right, Māori and Indigenous data sovereignty (IDSov) are closely aligned with other Indigenous rights set out in the United Nations Declaration on the Rights of Indigenous Peoples (UNDRIP) specifically Articles 3, 4, 5, 15(i), 18, 19, 20(i), 23, 31, 32, 33, 38, and 42 (for a more detailed analysis, see Davis, 2016, also see, Carroll, Rodriguez-Lonebear & Martinez, 2019). Governments that are signatories to the UNDRIP thus have responsibilities to think in more complex, nuanced ways about data jurisdiction and control. In Aotearoa, this also includes addressing Māori rights and interests under Te Tiriti.

Te Tiriti is widely accepted as Aotearoa's constitutional document that establishes and guides the relationship between Māori and the Crown. Article 2 of Te Tiriti guarantees the protection of iwi and hapū 'tino rangatiratanga' (chiefly authority) over their 'taonga katoa' (all treasured things). Both the Māori Data Sovereignty Network, Te Mana Raraunga,[18] and Te Kāhui Raraunga - the operational arm of the National Iwi Chairs Forum Data Iwi Leaders Group (Data ILG)[19] - have defined data as a taonga. In its report on *The comprehensive and progressive agreement for Trans-Pacific Partnership* (Wai 2522), the Waitangi Tribunal did not specify which kinds of data are taonga in their own right, but recognised that mātauranga Māori included Māori rights and interests in the digital domain and this placed "a heightened duty on the Crown to actively protect those rights and interests, particularly in a field that is subject to rapid change and evolution." It also recognised that "from a te ao Māori perspective, the way that the digital domain is governed and regulated has important potential implications for the integrity of the Māori knowledge system, which *is* a taonga" (Waitangi Tribunal, 2021, p.53).

A significant body of research on IDSov and MDSov provides an evidence base for the definition, operationalisation, and implementation of MDSov and IDSov. Studies in the so-called 'CANZUS' states (Canada, Australia, New Zealand, United States) have considered IDSov in relation to data governance (Carroll, Herczog, et al., 2021; Carroll, Rodriguez-Lonebear & Martinez, 2019), policy (Walter, Kukutai, Carroll & Rodriguez-Lonebear, 2020), open data (Rainie et al., 2019; Walter et al., 2021), health data (Griffiths et al., 2021; Walker et al., 2017), COVID-19 data (Carroll, Akee, et al., 2021; Yellowhorse & Huyser, 2021); and genomic data (Hudson et al., 2020; Tsosie et al., 2021). The CARE[20] principles for Indigenous data governance (Research Data Alliance International Indigenous Data Sovereignty Interest Group, 2019) have been endorsed by the Research Data Alliance – a global research community committed to research data sharing - and other international organisations and standards including UNESCO Recommendation on Open Science,[21] and the IEEE Recommended Practice on Provenance of Indigenous Peoples' Data.[22]

Upholding IDSov is not only seen as crucial for governments to meet their responsibilities towards Indigenous peoples, but an opportunity to transform data ecosystems to be more sustainable, generative, and socially just (Kukutai & Cormack, 2020; Walter, Kukutai, Carroll & Rodriguez-Lonebear, 2020; Lovett et al., 2019).

Of the six high-level Māori data sovereignty principles (Te Mana Raraunga, 2018), four are of particular relevance for considering issues of data storage and jurisdiction. They are:

1.1 (Rangatiratanga|Authority)
Control. Māori have an inherent right to exercise control over Māori data and Māori data ecosystems. This right includes, but is not limited to, the creation, collection, access, analysis, interpretation, management, security, dissemination, use and reuse of Māori data.

1.2 (Rangatiratanga|Authority)
Jurisdiction. Decisions about the physical and virtual storage of Māori data shall enhance control for current and future generations. Whenever possible, Māori data shall be stored in Aotearoa New Zealand.

3.2 (Whanaungatanga|Obligations)
Accountabilities. Individuals and organisations responsible for the creation, collection, analysis, management, access, security or dissemination of Māori data are accountable to the communities, groups and individuals from whom the data derive.

6.1 (Kaitiakitanga|Guardianship)
Guardianship. Māori data shall be stored and transferred in such a way that it enables and reinforces the capacity of Māori to exercise kaitiakitanga over Māori data.

The Special Rapporteur on the Right to Privacy (SRRP) has endorsed IDSov in two reports relating to big data and open data (Special Rapporteur on the right to privacy, 2018), and the protection and use of health-related data (Special Rapporteur on the right to privacy, 2019). In relation to data storage, the SRRP (2019, p. 27) acknowledges that:

Indigenous Peoples have the right to… ensure that the physical and virtual storage and archiving of Indigenous data enhances control for current and future generations of Indigenous Peoples. Whenever possible, Indigenous data shall be stored in the country or countries where the Indigenous People to whom the data relates consider their traditional land to be.

Taken together, this suggests that:

- onshoring should be the preferred option for storing Māori data, wherever possible and practicable;
- Māori should be actively involved in decisions regarding on/offshoring Māori data;
- MDSov should be incorporated into procurement policies and practices in relation to Cloud services;
- and decisions about the storage of Māori data should prioritise sustainability for future generations.

The current situation

To date, decision-making about offshoring government data has given little consideration to Te Tiriti obligations or MDSov requirements. An increasing number of government agencies are using offshore storage such as AWS or Azure, and/or cloud-based services running on public cloud platforms that are mostly located offshore (for a summary, see Bell Gully, 2021). For example, the Ministry of Health operates the COVID-19 immunisation register (CIR) that contains individuals' details including name, address, date of birth, ethnicity, National Health Index number and COVID-19 vaccination on a Salesforce platform which is hosted on AWS servers in Sydney.[23] Several Māori organisations have argued that CIR data should be repatriated to Aotearoa.[24] Only data classified as restricted or below is able to be stored in a cloud service, whether it is hosted onshore or offshore. It has been estimated that up to 95% of government data could be classified as restricted or below.[25]

Data ILG and Stats NZ have entered into a Tiriti-based Mana Ōrite agreement which recognises the equal authority of both parties to work together on data-related projects that make a "sustainable positive difference to outcomes for iwi, hapū and whānau."[26] One of the projects involves the co-design of a Māori data governance model using a waka hourua (double-hulled canoe) framework (Te Kāhui Raraunga, 2021a, 2021b).[27] Intended as an AOG approach, the waka hourua model is unlikely to address, in detail, the specific issue of data storage and processing so separate guidance will likely be needed. A separate Mana Ōrite agreement was also signed between Data ILG and the Department of Internal Affairs in June 2021.[28] DIA is the Government's functional lead agency for digital public services, including cloud-services, so the agreement provides an opportunity for a partnered approach to decision-making on offshoring of Government data.

Both Statistics NZ - as the government's functional lead for data and analytics[29] - and DIA are seeking to better understand Māori perspectives and concerns about offshoring. Statistics NZ commissioned Bell Gully to produce the report Offshoring New Zealand Government data, which provides a range of perspectives on the benefits and risks of onshore and offshore data storage through a Te Tiriti and te ao Māori lens. The paper came about, in large part, because of concerns raised by the Data ILG about the Government offshoring Māori data. The report stops short of making specific recommendations but does suggest that a desirable course of action would be for Māori and agencies to work together to "co-design a framework, to be used by all agencies, to facilitate a weighing-up of the risks and benefits of offshoring on a case-by-case basis" (Bell Gully, 2021, p. 10).

Given the Article 2 guarantee of tino rangatiratanga, and the principles of partnership and options, the report argues that Māori should be involved in making decisions about the storage of Māori data and data governance more generally. While it may not be practical to invoke consultation every time a classification or on/offshoring decision is made, there is considerable scope to co-design a framework that could be applied by agencies making decisions about data storage. The aim of such a framework would be to "provide a set of guidelines about how certain types of data should be handled, and the circumstances in which additional input (consultation, or shared decision making) from Māori should be sought." Bell Gully's report also notes that "if the government is to have a conversation with Māori around data location, there is a need to consider how agencies make decisions regarding the procurement and use of onshore and offshore cloud-based services more generally" (p. 4). With regards to data as a taonga, the report notes that, "In the context of Māori data, active protection would seem to us to require at the very least that the data is held securely and that it is protected for future generations." In determining what data is a taonga, the nature and value of the taonga, and how it should be protected, agencies should be guided by Māori.

We next consider how different offshoring options might align, or be in tension with, MDSov requirements.

Aotearoa options for cloud

For Aotearoa to give expression to MDSov, it warrants taking a broad perspective of the options for cloud. While the list below is not definitive, there are certainly more options than the prevailing mono view:

- public cloud (offshore) e.g., a foreign-owned offshore-hosted provider;
- public cloud (onshore) e.g., a locally-owned, locally-hosted provider;
- public cloud (onshore) e.g., a foreign-owned, locally-hosted provider, such as Microsoft's promised Azure data centre in Auckland and AWS also in Auckland;
- private or community cloud (onshore) e.g., Māori-owned, Māori hosted;
- hybrid or multi cloud (onshore) e.g., public and private cloud both onshore;
- hybrid or multi cloud (onshore/offshore) e.g., private cloud onshore/public cloud offshore;
- non-cloud (Māori federated or bespoke).

The assumption that locally-owned and locally-administered cloud solutions are always less secure and reliable than overseas ones (Bell Gully, 2021) needs testing. We do not believe this is inevitably true, nor that it will inevitably remain true. Even if it is true now, there may be substantial benefits to investing in local infrastructure capacity rather than choosing an overseas provider as the default option, particularly if there is an obligation to take account of MDSov requirements. Having a proactive approach to strengthening local infrastructure also aligns with calls for additional investment in developing local workforce capability to lift Aotearoa's global competitiveness.

There may also be many more important questions than, "offshore or onshore?" One of the issues that gets lost in the debate is the use of third-party Software-as-a-Service (SaaS) services and where the data using these services are hosted/stored.

Examples include:

- map data (user generated data such as pins, or claim a business location e.g., Google Maps);
- messaging data (peer to peer messaging in event apps e.g., Attendify);
- forms (user generated e.g., Google forms);
- bulk email communications (e.g., MailChimp);
- bulk SMS messaging (e.g., Twilio);
- websites (e.g., Squarespace, WIX, Weebly);
- email data.

Depending on data categorisation such as sensitive data, there may be no adequately secure cloud storage solution. The right answer to "should we store this data in Internet-accessible cloud storage onshore or offshore?" may be "neither." Some data should not be in Internet-accessible cloud storage. This is particularly relevant when there is no need for the data to be remotely accessible, or when the data owners have not been asked what they would prefer.

Other than scale and cost, the difference between onshore and offshore providers may also be less important than other issues such as ownership or outsourcing. A foreign-owned but locally situated provider is like an offshore provider in many ways – or an extension, such as AWS or Azure Edge. Conversely, a locally-owned and locally-hosted provider that makes an offshore backup is subject to all the risks of offshoring.

It is also helpful to distinguish between the different options for data storage and processing with respect to Infrastructure-as-a-Service (IaaS),[30] Platform-as-a-Service (PaaS)[31] and SaaS.[32] IAAS options such as Microsoft Azure and AWS provide administrators with more direct control over operating systems. PaaS provides cloud components to certain software while being used mainly for applications. Examples include Windows Azure and the Google app engine affording users greater flexibility and ease of operation. SaaS, also known as cloud application services, are accessed over the intent and hosted on a remote server. Well-known examples include Salesforce and Dropbox. We also consider which technologies - specifically, encryption - would help to reduce some of the risks associated with offshoring.

Technology

When evaluating the risks and benefits of offshoring of data, it is important to not only consider data storage, but also broader issues related to offshore data processing. Effective use of a cloud provider, whether onshore or offshore, is unlikely to *only* involve data storage. In such scenarios it would require the repatriation of all the data prior to any processing taking place on it, which is clearly impractical in terms of time and cost. As such, the typical paradigm will involve data processing taking place in the same environment as where the data is stored.

It is therefore important to consider the implications of processing as well as storage. This has a potentially profound impact on the assumptions associated with encrypting the data. Whilst it would theoretically be possible to encrypt data locally and store it offshore, in practical terms this would be of little use other than for back-up. The same issue of having to repatriate to decrypt and process the data would exist. As such, the decryption key would normally be stored with or accessible by the processing devices offshore. This significantly changes the trust assumptions and where sovereignty of access ultimately lies.

As such, it is important to ensure that even when looking primarily at data storage, the corresponding processing that would be expected to be accompanied is considered. For example, it would be incorrect to assume that IaaS is solely related to data storage, when it includes data processing as well. To aid in this regard we provide a detailed clarification of the technologies that can be deployed, and the protections afforded to the data.

IaaS vs. PaaS vs. SaaS

The simplest way of differentiating between these models is not based on functionality but *responsibility*. IaaS can provide similar, or even identical, functionality as SaaS. However, who is responsible for different parts is very different. Microsoft describes the various approaches through a shared responsibility model, as shown in their illustration in Figure 1.

IaaS provides the greatest flexibility but also the greatest responsibility for the user (usually a systems administrator). It is the user's responsibility to install, configure and maintain everything from the operating system upwards. The network configuration is also often the responsibility of the user. With PaaS a portion of the responsibility is shifted to the provider, normally the provision of a core set of software or frameworks, for example, the operating system or development frameworks. The user is still responsible for maintaining and updating the applications they install or deploy, but the underlying platform will be maintained by the provider. Beyond that, SaaS shifts almost all responsibility for infrastructure to the provider. The user is responsible for some basic configuration, but the full software stack is maintained by the provider.

Shared responsibiltiy model

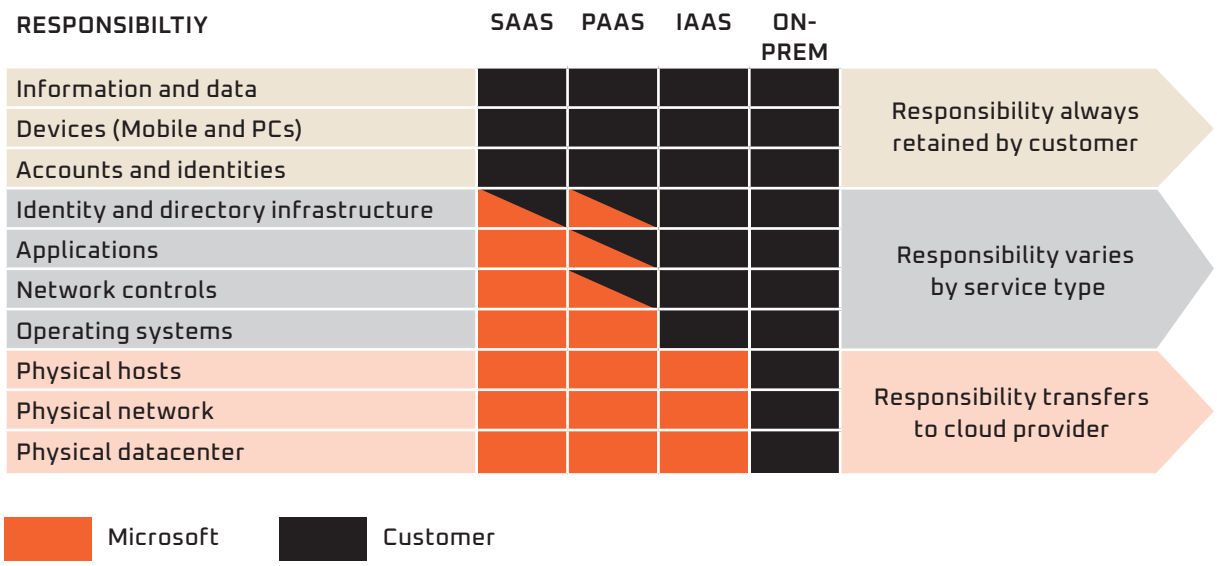

Figure 1: Microsoft Azure Shared Responsibility Model

This distinction is crucial in an environment believed to have a capability gap. Deploying applications and services on IaaS without having the necessary security capability within the deploying organisation can lead to vulnerabilities such as security misconfigurations and/or subsequent breaches. IaaS does not provide an inherent security benefit out of the box. For example, Amazon S3, a hugely popular data storage product, has become notorious for misconfigurations leaking gigabytes of data about millions of individuals.[33] Some of the most recent egregious examples are the 540 million Facebook app records found to be publicly accessible in 2019,[34] the millions of Verizon customer records in 2017,[35] or the 1.8 million voter records from Chicago in 2016.[36] These are not isolated incidents - there are top 10 lists of the worst S3 breaches.[37]

That is not to say that there is an inherent problem with Amazon AWS or the S3 service. IaaS does not guarantee security even if deployed on one of the leading cloud providers. It is also not limited to just storage provisions. IaaS in general is considered to be a source of a large number of under-reported security breaches.[38]

Security misconfigurations are also not limited to IaaS. PaaS and SaaS offerings have also suffered similar misconfigurations leading to large scale breaches. Elastic Search, whether hosted on AWS or via the ElasticCloud, has been the source of a number of such breaches, including the nearly 57 million records of US Citizens[39] or the 1.2 billion individual records found to be publicly available.[40] Similarly, Google Firebase, a hosted and managed database that has been referred to as a Backend-as-a-Service - similar to SaaS but targeting developers - suffered from widespread misconfigurations that were found to impact on thousands of databases and millions of records, some of which were sensitive medical records.[41]

It should also be noted that in all of the above cases the cloud providers made available sophisticated tools and options to protect and monitor deployments. It is perfectly possible to safely deploy such services and applications in a cloud. However, to achieve that requires local capability, and as such, organisations must be extremely cautious if they are moving to cloud infrastructure as a way to bridge a capability gap. They may well find the gap remains, but with the service now at arm's length, the vulnerabilities may be even greater and harder to detect.

Control shifts with responsibility

When shifting responsibility for infrastructure management to a provider, for example, by utilising PaaS or SaaS options, there is also a transfer of control of the data. There will of course be contractual limitations, but fundamentally, the provider is the system administrator and should be considered to have the same access as a local system administrator would have had in an onsite deployment. As such, security assessments should be evaluated within that context, and make clear the additional transfer of trust that accompanies the data to the provider.

IaaS vs. storage and encryption

It is important not to conflate IaaS and storage. IaaS provides more than just storage capabilities - it is most commonly considered to provide compute power. Whilst it is true that the use of local encryption prior to storage overseas would address many concerns about access and security, such a use case is unlikely to materialise in practice. Crucially, such an approach precludes processing the data on the infrastructure overseas.[42] As such, each time the data needs to be accessed or processed it must be repatriated to Aotearoa, decrypted, and then processed on local infrastructure. Similarly, if the data was encrypted during transit, requiring the encryption keys to be held in Aotearoa would have the same net result. This is extremely inefficient in terms of bandwidth and latency. If government data are offshored using IaaS, it is likely that data will not only be stored, but also are *processed*, in the overseas cloud. In order to do that the decryption key must reside in the cloud infrastructure overseas and, as such, the security and privacy of the data is greatly reduced.

Jurisdictional risk

In the last decade there have been several government reports addressing aspects of jurisdictional risk (see, for example, Minister of Internal Affairs, 2016; New Zealand Government, 2017). When evaluating jurisdictional risk, it is important to consider the issue more broadly than merely where the data centre is located. Such an evaluation over simplifies the challenge in the presence of legislation that exists in a number of relevant countries. For example, both the USA and China assert jurisdiction over data stored by companies headquartered in their respective countries. Much of the associated legislation is relatively new, contentious, or untested, and as such creates significant ambiguity in determining privacy risk of data stored on platforms run by companies headquartered overseas.

One example of a contemporary and relevant analysis is Greenleaf and Kemp's (2020, p. 6) discussion of the implications of Australia's COVIDSafe data being stored in an Amazon cloud service located in Australia.

There are circumstances where the US Clarifying Lawful Overseas Use of Data Act (2018) (CLOUD Act) could be used to compel Amazon Web Services (AWS), as a provider of a remote computing service that is subject to US jurisdiction, to disclose the contents of a record to the US government even if the record is located outside the US. At this stage, AWS is not entitled to bring a motion to quash or modify that legal process in a US court, on the basis that disclosure would contravene a law of Australia, since the Australian government is not a "qualifying foreign government" under the CLOUD Act. Home Affairs Minister Dutton introduced a bill in March 2020 (the IPO Bill) essentially to allow Australian and US law enforcement agencies to reciprocate and cooperate in obtaining access to communications and records under the CLOUD Act processes. If the IPO Bill is passed, the Australian government may become a "qualifying foreign government" under the CLOUD Act. Greenleaf and Kemp's (2020, p.6).

An answer to the question of whether records held by AWS as part of its COVIDSafe contract would be subject to the US CLOUD Act or the IPO Bill is not straightforward.

Greenleaf and Kemp discussed the specific case of data stored in an AWS data center located within the storing nation's territory, namely Australia, and the impact of the US CLOUD Act on its security and privacy. However, this is by no means an isolated case, and warrants issued in the US demanding access to data housed overseas are also not purely theoretical. By examining the transparency report of a similar provider, Microsoft, we can see that in the first half of 2021[43] there were 27,809 legal demands for access to consumer data, of which 21,417 sought data that was stored outside of the USA. While the foregoing paper discusses the impact of US law on data stored on a US-owned cloud in Australia, it is likely that the UK's Investigatory Powers Act, Australia's Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018, and equivalent legislation in authoritarian countries including China, would imply similar jurisdictional risk for data centres controlled by their respective countries, even if located in Aotearoa.

Another important source of jurisdictional risk is data in transit between Aotearoa and an offshore cloud service. Both the US[44] and the UK[45] permit bulk interception of communications originating overseas - which would be the case for Aotearoa Government data. As such, the transfers could be susceptible to routine bulk interception. In effect, the data coming from Aotearoa could be offered a lower level of protection than data originating within the country. How the data is transmitted, how it is stored, and how it will be used is crucial, as are the specific legislative and interception regimes that exist in the various countries.

The risk of bulk interception is substantially reduced by local storage. It is not completely eliminated because traffic within one country can still be misdirected outside it by manipulating the internet's routing protocols.[46]

The foregoing risks have not been transparently discussed in any depth by the New Zealand Government. Guidelines on managing jurisdictional risk for public cloud services (New Zealand Government, 2017) did not include a country-by-country analysis – only agencies had access to the risk assessments in 8 jurisdictions including the US, UK, Singapore and Australia. Whilst public access may not be appropriate for diplomatic reasons, the lack of detailed information makes it very difficult for Māori, as Tiriti partners, to properly assess risk in order to make decisions about the offshoring of their data. Indeed, we have not yet been able to locate any publicly available report that provides the depth of information required for Māori to reliably assess jurisdictional risks and associated issues of data residency and localisation.[47]

Information security risk

Data location is key for assessing jurisdictional risk, but it also needs to be considered when assessing security risk. Location is not entirely absent from information security risk. Issues such as the availability of cyber security skills in that jurisdiction, the maturity and enforcement of associated protections, the history and prevalence of attacks or unauthorised access in that location, all impact information security risk.[48] As part of the cloud first policy refresh, what assessment or certification of cloud service providers will the required to ensure information security standards are met? We note here the requirement under the Privacy Act 2020 for notifiable privacy breaches to be notifed to the Office of the Privacy Commissioner within 72 hours of becoming aware of the breach.

Integrity

Integrity refers to the possibility for the data to be accidentally or deliberately corrupted. In this case, the risks for integrity are approximately the same as the information security risk. It seems important to establish by careful examination whether all locally-owned providers really are less secure than larger international ones.

Availability

Too often it is assumed that reliability and redundancy (data storage in two or more separate places to avoid a single point of failure) can only be assured by overseas providers. However, overseas providers are not immune from failures or collapse. For example, in December 2020 Google services suffered a global outage.[49] In 2021, two of the biggest outages included cloud providers AWS and Azure. Two Facebook outages also featured among the top 10 outages.[50] The evaluation of overseas providers should take account of whether suitable redress or priority can be obtained should such an event occur.

There is a clear advantage to replicating data off-site and out of region. However, data replication, as described above, can be done more securely than data processing, for example by storing a backup encrypted with a key known only to the data owner. As such, a local provider could obtain significant data redundancy by using locally encrypted backups that are stored overseas, but would still be protected from interception or unauthorised access. That is a very different prospect to deploying processing overseas.

More importantly, whilst the infrastructure overseas offers greater redundancy, access to that infrastructure does not have the same redundancy. There are only five undersea cables[51] connecting Aotearoa to the rest of the world. Two of them are connections to Australia, two are to the US and Australia, and one is to just the US.

The loss of any of these cables, whether deliberately or through a natural disaster, could significantly impact on the ability to access overseas infrastructure. Therefore the data's location matters to the risk of unavailability. Where are the dependencies and what countries must the data travel through? How much bandwidth capacity exists and what redundancy is there? Is there a local cache?[52] Losing access to essential data, even temporarily, could be critical. The breaking of undersea cables is relatively common - mostly caused by accidental damage in shallow waters. However, future malicious intent from foreign powers cannot be ruled out as a possibility.[53]

The ability to rapidly scale and recover from a disaster is seen as a benefit of overseas providers (Bell Gully, 2021, p. 57), but there is no evidence to suggest that is the case. Should an overseas provider cease trading, the ability to recover data is not guaranteed. Moving data out of one provider to another is a time consuming task, often taking weeks or months when data is stored at scale.[54] The ability to influence procedure or protect interests overseas is obviously diminished in comparison to domestic-based organisations. In a crisis where will Aotearoa be in the priority list in terms of safeguarding or accessing its data? Service level agreements normally cease being enforceable once a company enters bankruptcy. What evidence is there that suitable provisions will occur in the event of a crisis?

Security and sovereignty

HERE WE CONSIDER TWO KEY QUESTIONS:

1. Are all local providers inevitably less secure than the offshore options? i.e. is local storage really less reliable?
2. What are the likely implications for Māori influence on decision-making of choosing a big multinational vs a NZ-owned company?

Presently it is unclear which options would give the greatest role to Māori holders of the data, but we see no reason to assume that a locally-hosted Microsoft Azure solution would be the only, or even the most likely, to give Māori a "central role" (Bell Gully, 2021, p. 52).

There are multiple examples of local providers, providing appropriate solutions across Aotearoa and to marae, hapū, iwi, and Māori. It would appear however, that when considering large amounts of data, such as Government or 'public' data, the ability to scale (up or down) and associated economics becomes a key consideration and the benefits of hyperscale cloud (currently available offshore through AWS, Azure and Oracle as examples) receive more attention.

There might be incentives for a local provider to be a lot more responsive to local requirements, including more incentive to build a good relationship with iwi and Māori, rather than simply applying a pre-packaged solution. We think this point deserves much more weight and consideration, particularly responsiveness to MDSov requirements, for example, by asking both Microsoft and potential local providers for firm undertakings and commitments before contract signing.

The issue of ownership is complex, but this also extends to consent. A US centric approach views data as a commodity that the individual is free to sell or exchange, whereas a European Union approach sets minimum protections/rights that an individual cannot consent to waive. The issue becomes more complicated with individual data that allows inferences about others, a primary example being DNA. Whilst someone's DNA is unique to them, and in the US model could therefore be treated as a commodity, it also provides insight into past, present, and future generations. As such, any sale or transaction on that data impacts more than just the individual. The challenge of how to manage and protect such data has so far remained unresolved, but Māori notions of shared control and interest could help shape an issue that impacts Indigenous peoples more widely (Beaton et al., 2017; Tsosie et al., 2021). As such it is vital to consider such data and how best to manage it and to learn lessons on the structures and processes associated with shared control and protection. The current government security classification is not sufficiently nuanced to adequately capture various stakeholders (Bell Gully, 2021). We would go beyond that and argue that existing approaches for evaluating privacy and consent may also be insufficient and a new paradigm that considers collective rights should also be considered.

While it is assumed that there is a skills gap and lack of maturity in onshore solutions - it is difficult to see how the current approach will help address it, and more importantly, how it will address the associated Māori skills gap. The collection, storage and processing of data is not going to decline in the future. As such, favouring short-term benefits over longer term capability is unwise. The skills gap will only be addressed if there is a suitable job market, which is unlikely to materialise if all the data is stored and processed overseas. More strategically, creating a systemic dependence on overseas companies for critical infrastructure and services seems short-sighted. It ignores both the possibility for a local multinational (Microsoft Azure) and significant variation in the quality of local providers.

A summary of pros and cons

Below we summarise some of the relative strengths of different options for cloud. Any summary is an oversimplification, leaving plenty of room for alternative interpretations or priorities. We simply make the point that the offshore, foreign-owned solution is not nearly as overwhelmingly advantageous as the current Government discourse makes it seem.

1. **Security—capability and maturity**

   The capability and maturity of foreign owned services would be expected to be stronger than onshore offerings. We do not believe this to be an absolute—onshore offerings are not inherently insecure and continue to develop.

2. **Security—data-in-transit**

   Data-in-transit faces greater threats when travelling over foreign networks, whether those threats are to security or availability. As such, offshore options are less favourable. We consider the onshore options to be largely equal on the basis that securing data-in-transit is sufficiently commonplace that it would not be impacted by differences in local capability.

3. **Security—cyber**

   The provision of advanced tools does not guarantee they are correctly deployed or configured. There is still a dependency on local capability. We do not distinguish between on and offshore foreign owned provisions since the entire argument for them is replication of function, so we don't consider a foreign owned onshore provision to be weaker than an offshore foreign owned provision.

4. **Jurisdictional risk—data at rest**

   The lowest jurisdictional risk is with a locally owned onshore provision, with the highest risk being an offshore foreign owned provision. The differentiator is not solely location—an onshore foreign owned provision will still be subject to data access laws in the country of origin of the provider. This is particularly significant when considering trade agreements that may include Māori data which is considered a taonga and any associated mātauranga Māori or cultural values implicit in the data.

5. **Jurisdictional risk—data in transit**

   Some countries provide less protection for foreign-sourced data in transit to or through them, than data at rest in them. This risk is less for onshore solutions, though it is still possible to misdirect traffic within a country through an alternative path outside that country.

6. **Stability of service provision/availability**

   Offshore providers have also suffered outages. Furthermore, there is an availability risk posed by the dependence on undersea cables.

7. **Access control transparency**

   We consider access controls and risk of access by service providers to be two separate issues. We consider greater oversight to be probably more easily achievable in onshore solutions, even more so with locally owned providers.

8. **Risk of access by services provider**

   We do not see a significant difference in risk associated with service provider access. This is a fundamental tenet of cloud provision: you are trusting the provider with your data. That is largely unavoidable.

9. **Business continuity/back-ups**

   There is considerable risk associated with overseas deployments from connectivity issues as we have previously outlined. Suitable data redundancy can be achieved without risking security or privacy through the use of local encryption. There are no perfect solutions, we consider all capable of providing redundancy and all facing vulnerabilities to that redundancy.

10. **Latency**

    Clearly an offshore solution is going to face greater latency issues. There is also a longer term concern with whether suitable bandwidth capacity will always be available in the future.

11. **Lower cost**

    We assume there will be economies of scale that benefit foreign owners, both in terms of existing overseas infrastructure and in its replication onshore.

12. **Service provider maturity**

    Whilst it is true that offshore providers have greater maturity, it seems clear that it is desirable for the local skills gap to be closed, and that government policy should assist in that regard, rather than perpetuating the problem by not supporting local development.

13. **Market maturity**

    We consider this to be of equal value to all. A new player benefits from previous hardware development and the commodification of server equipment. Likewise, many software developments have taken place in open source solutions, ElasticSearch, OpenStack, etc. all of which would benefit a developing local organisation that would not need to reinvent the wheel.

14. **Potential for vendor lock-in**

    The issue of vendor lock-in is a concern across all providers. Usage of open source technology and solutions can mitigate such risks, something that is often not possible with offshore foreign owner provisions.

    The prospect of vendor lock-in may be exacerbated if locally-owned providers are pushed out of the market, e.g. by Microsoft's local Azure cloud.

15. **Capability building**

    The necessity to manage and process data is not going to disappear. That is a capability that is essential to industry and government. Policies should support the local building of that capability and not prioritise short-term gains that may create long-term systemic dependencies on foreign providers.

16. **Māori co-design**

    We are not certain of the opportunities for Māori determination of data use for any of these options, but it seems much more likely with a locally owned provider or an onshore provider who is responsive to UNDRIP in other jurisdictions and locales and therefore more likely to be receptive to co-design with Māori.

Conclusion

As the government accelerates its digital transformation strategy across the public service, MDSov requirements must be central to decision making, particularly with regard to offshoring and procurement. This requires a more considered, intergenerational approach to data stewardship than the current narrow focus on assessing offshoring risks and benefits.

Strategic investment in locally-hosted options would not only give greater effect to MDSov, but also enhance the public service drive for digital transformation. In that regard MDSov is not about siloing Māori data and deciding what to 'do' with it based on a matrix of tick-box type questions and responses. Rather, MDSov offers a more holistic, tikanga-led approach to treating data that is inherently relational, that cannot be reduced to personal data rights and protection, and that is about driving towards better data relationships for all.

WE OFFER FOUR HIGH-LEVEL RECOMMENDATIONS:

Recommendation 1	Recommendation 2	Recommendation 3	Recommendation 4
Māori Influence over Policy & System Decisions	**Māori Influence over AOG Cloud Procurement**	**AOG Cloud Service Agreements recognise Māori Data Sovereignty**	**Strategic Investment in wider options to give effect to Māori Data Sovereignty**

1. **That Māori, as a Tiriti partner, are involved in policy setting and system-level decisions regarding the digital public service transformation across key public sector agencies (if not all).**

   We suggest a two-pronged approach:

   (i) Leveraging the Mana Ōrite relationships, Māori lead the development of Māori data classification to drive policy and inform/reform legislation, including mechanisms such as the Cloud First Policy refresh, and any bilateral negotiations between the New Zealand Government and other jurisdictions relating to data or digital technology transformation. It might also include tools for assessing onshore/offshore suitability with relative weighting of factors determined by iwi and Māori. Involvement at a system level requires intentional line of sight to understand the implications for implementation and operationalisation.

   (ii) Iwi and Māori exercise their own tino rangatiratanga and mana motuhake directly with cloud service providers to influence the indigenising of their services for Māori and Indigenous peoples globally.

2. **That Māori, as a Tiriti partner, are involved in system-level decisions regarding AOG procurement policies and use of onshore and offshore cloud-based services.**

   The oft cited 'what's good for Māori, is good for all New Zealanders' resonates as it will require the development of more inclusive AOG procurement policies and practices, and lift the interrogation of services to deliver equitable outcomes for all of Aotearoa.

   The ability to respond to a framework for Māori data is a mandatory assessment requirement incorporated into EOIs and RFPs as part of AOG procurement practice seeking data or digital technologies services. This could be ably supported by the establishment of a MDSov Assessment panel comprised of a combination of Māori Data Governance panel members (advisors to GCDO) and individual Māori assessors drawn from a pool of Māori ICT practitioners (similar to the MBIE College of Assessors model[55]) with requisite pūkenga across data, infrastructure, Cloud services, middleware, applications, mobile, cybersecurity etc.

3. **That MDSov requirements are developed and incorporated into contractual agreements such as Master Service Agreements (e.g., Cloud Framework Agreements) for the use of onshore and offshore cloud-based services.**

   These umbrella agreements provide standard terms and conditions for the procurement of goods or services and will often seek a 'win-win' outcome recognising value in the relationship. This is consistent with iwi and Māori relational worldview. If a requirement of AOG Procurement includes provisions relating to MDSov as recommended above, there are fewer surprises at the time of contracting. An added benefit for cloud service providers might be extending thinking to other Indigenous peoples as customers and deriving innovative approaches in other contexts.

4. **That there is strategic infrastructure investment in a wider range of options to enable both Tangata Whenua and Tangata Tiriti partners to give effect to MDSov.**

   The opportunity space as envisaged in Te Tiriti invites a range of options be considered and this extends to MDSov. The Government should actively seek options for iwi and Māori to exercise their mana motuhake over their taonga called data and provide strategic infrastructure investment beyond public cloud (offshore) to include public cloud (onshore), hybrid or multi cloud (onshore/offshore), private or community cloud (Māori-owned, Māori-hosted onshore storage solutions or fit for purpose arrangements with Te Tiriti-led cloud service providers). This might also include the establishment of Māori 'data islands' within Aotearoa (Bell Gully, 2021, p.68).

   Such strategic investment will likely require the public sector to review existing legislation and planned AOG policies and to develop new policies or respond to MDSov in new ways. It will likely require cloud service providers to advance their thinking and responsiveness to UNDRIP. The impact on existing data and digital trade agreements will also require recasting MDSov in relation to data, cultural IP, and mātauranga.

   Finally, existing negotiations such as Aotearoa's accession to the Budapest Convention and associated legislative reform, along with negotiations of any proposed CLOUD Act bilateral between Aotearoa and the USA, should incorporate MDSov in ways that are informed by and with iwi and Māori.

References

Beaton, A., Hudson, M., Milne, M., Port, R. V., Russell, K., Smith, B., ... & Wihongi, H. (2017). Engaging Māori in biobanking and genomic research: a model for biobanks to guide culturally informed governance, operational, and community engagement activities. *Genetics in Medicine, 19*(3), 345-351.

Bell Gully (2021). *Offshoring New Zealand Government data. A report prepared for Statistics New Zealand*. Wellington: Bell Gully.

Bilgic, S. (2018). Something old, something new, and something moot: The privacy crisis under the CLOUD Act. *Harv. JL & Tech.*, 32, 321.

Carroll, S. R., Rodriguez-Lonebear, D. & Martinez, A. (2019). 'Indigenous Data Governance: Strategies from United States Native Nations', *Data Science Journal, 18*(31), pp. 1-15.

Carroll, S. R., Herczog, E., Hudson, M., Russell, K., & Stall, S. (2021). Operationalizing the CARE and FAIR Principles for Indigenous data futures. *Scientific Data, 8*(1), 1-6.

Carroll, S. R., Akee, R., Chung, P., Cormack, D., Kukutai, T., Lovett, R., ... & Rowe, R. K. (2021). Indigenous peoples' data during COVID-19: from external to internal. *Frontiers in Sociology, 6*, 62.

Cormack, D., Kukutai, T., & Cormack, C. 2020. Not one byte more. In A. Chen (ed), *Shouting zeros and ones: Digital technology, ethics and policy in New Zealand* (pp. 71-83). Wellington: Bridget Williams Books.

Davis, M. (2016). Data and the United Nations Declaration on the Rights of Indigenous Peoples. In Kukutai, T. & Taylor, J. (Eds.) (2016). *Indigenous data sovereignty: Toward an agenda* (pp. 25- 28). Canberra: ANU Press.

Greenleaf, G. & Kemp, K. (2020). *Australia's 'COVIDSafe' App: An experiment in surveillance, trust and law*. University of New South Wales Law Research Series, 999. Retrieved from https://ssrn.com/abstract=3589317

Griffiths, K. E., Blain, J., Vajdic, C. M., & Jorm, L. (2021). Indigenous and Tribal Peoples data governance in health research: A systematic review. *International Journal of Environmental Research and Public Health, 18*(19), 10318.

Hawaiiki NUI https://www.stuff.co.nz/business/126851934/huge-subsea-internet-cable-will-boost-south-islands-digital-economy

Hudson, M., Garrison, N., Sterling, R., Caron, N. Fox, K., Yracheta, J., Anderson, J. et al. (2020). Rights, interests and expectations: Indigenous perspectives on unrestricted access to genomic data. *Nature Reviews Genetics, 21*(6), 377-384.

Kukutai, T. & Cormack, D. (2020). "Pushing the space": Data sovereignty and self-determination in Aotearoa NZ. In M. Walter, T. Kukutai, S. Russo Carroll & D. Rodriguez-Lonebear (eds), *Indigenous data sovereignty and policy*. London: Routledge.

Kukutai, T. & Taylor, J. (Eds.) (2016). *Indigenous data sovereignty: Toward an agenda*. Canberra: ANU Press.

Lovett, R., Lee, V. Kukutai, T., Cormack, D., Rainie, S. & Walker, J. (2019). Good data practices for Indigenous data sovereignty and governance. In A. Daly, K. Devitt & M. Mann (eds), *Good data*. Amsterdam: Institute of Network Cultures.

Mann, M., Daly, A. & Molnar, A. (2020). Regulatory arbitrage and transnational surveillance: Australia's extraterritorial assistance to access encrypted communications. *Internet Policy Review, 9*(3), 1-20.

Minister of Internal Affairs (2016). *Accelerating the adoption of public cloud services*. Wellington: Office of the Minister of Internal Affairs. Retrieved from https://www.digital.govt.nz/dmsdocument/15-accelerating-the-adoption-of-public-cloud-services/html

New Zealand Government (2020). *Strategy for a Digital Public Service*. Wellington: New Zealand Government. Retrieved from https://www.digital.govt.nz/digital-government/strategy/strategy-summary/strategy-for-a-digital-public-service/

New Zealand Government (2017). *Managing jurisdictional risks for public cloud services version 1.0*. Wellington: New Zealand Government. Retrieved from https://snapshot.ict.govt.nz/resources/digital-ict-archive/static/localhost_8000/assets/Guidance-and-Resources/Cloud-ICT-Assurance/Jurisdictional-risks-v1.0-UNCLASSIFIED.pdf

Rainie, S., Kukutai, T., Walter, M., Figueroa-Rodriguez, O., Walker, J. & Axelsson, P. 2019. Issues in open data: Indigenous data sovereignty. In T. Davies, S. Walker, M. Rubinstein & F. Perini (eds), *The state of open data: Histories and horizons*. Cape Town and Ottawa: African Minds and International Development Research Centre. doi:10.5281/zenodo.2677801

Research Data Alliance International Indigenous Data Sovereignty Interest Group. (2019). *CARE Principles for Indigenous data governance*. Retrieved from https://www.gida-global.org/care

Southern Cross NEXT https://www.scoop.co.nz/stories/HL2205/S00029/the-download-weekly-southern-cross-next-cable-live-in-july.htm

Special Rapporteur on the right to privacy (2018). *Big data and open data taskforce report (A/73/438)*. Retrieved from https://www.ohchr.org/en/calls-for-input/reports/2018/report-big-data-and-open-data

Special Rapporteur on the right to privacy (2019). *Report on the protection and use of health-related data (A/74/277)*. Retrieved from https://www.ohchr.org/en/calls-for-input/reports/2019/report-thee-protection-and-use-health-related-data

Te Kāhui Raraunga (n.d.). *Iwi data needs*. Retrieved from https://www.kahuiraraunga.io/iwidataneeds

Te Kāhui Raraunga (2021a). *Tawhiti nuku. Māori data governance co-design outcomes report*. Rotorua: Te Kāhui Raraunga.

Te Kāhui Raraunga (2021b). *Māori data governance co-design review*. Rotorua: Te Kāhui Raraunga.

Te Mana Raraunga (2018). *Principles of Māori data sovereignty*. Retrieved from https://www.temanararaunga.maori.nz/nga-rauemi

Tsosie, K. S., Yracheta, J. M., Kolopenuk, J. A., & Geary, J. (2021). We have "gifted" enough: indigenous genomic data sovereignty in precision medicine. *The American Journal of Bioethics, 21*(4), 72-75.

Waitangi Tribunal (2021). *The comprehensive and progressive agreement for Trans-Pacific Partnership (Wai 2522)*. Wellington: Waitangi Tribunal.

Walker, J., Lovett, R., Kukutai, T., Jones, C., & Henry, D. (2017). Indigenous health data and the path to healing. *Lancet, 390*(10107), 2022-2023.

Walter, M. Kukutai, T., Carroll, S. R. & Rodriguez-Lonebear, D. (Eds.) (2020). *Indigenous data sovereignty and policy*. London: Routledge.

Walter, M., Lovett, R., Maher, B., Williamson, B., Prehn, J., Bodkin-Andrews, G., & Lee, V. (2021). Indigenous data sovereignty in the era of big data and open data. *Australian Journal of Social Issues, 56*(2), 143-156.

Yellow Horse, A. J., & Huyser, K. R. (2021). Indigenous data sovereignty and COVID-19 data issues for American Indian and Alaska Native Tribes and populations. *Journal of Population Research*, 1-5.

Endnotes

[1] Data Iwi Leaders Group technician *Tahu Kukutai*, Prof, Te Ngira: Institute for Population Research, University of Waikato *Vanessa Clark*, Te Kāhui Raraunga Technician and Research Developer (Māori Engagement), Research and Enterprise, University of Waikato

[2] Principal, Castellate Consulting Ltd., chris@castellate.com

[3] CEO, Thinking Cybersecurity Pty Ltd., and A/Prof (Adj.), Australian National University, vanessa@thinkingcybersecurity.com

[4] https://snapshot.ict.govt.nz/guidance-and-resources/using-cloud-services/why-agencies-must-use-cloud-services/index.html

[5] https://www.digital.govt.nz/digital-government/leadership/government-functional-leads/government-chief-digital-officer-gcdo/; also, https://www.digital.govt.nz/standards-and-guidance

[6] https://www.digital.govt.nz/standards-and-guidance/technology-and-architecture/cloud-services/

[7] Assessment of jurisdictional risk include taking account of how foreign governments lawfully access data which is stored, processed, or transmitted in their territory, as well as how cloud services providers respond to requests by other governments for access to the data they store, process or transmit (New Zealand Government, 2016).

[8] https://www.newsroom.co.nz/australias-new-encryption-law-threatens-nz-cloud-data We also note that the New Zealand government recently joined the Council of Europe Convention on Cybercrime (the Budapest Convention) which is the sole legally binding international multilateral treaty on cybercrime, and allows for a much higher degree of data sharing between nation-states in relation to cybercrime investigations.

[9] https://www.justice.gov/opa/pr/us-and-uk-sign-landmark-cross-border-data-access-agreement-combat-criminals-and-terrorists

[10] https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/australia-united-states-cloud-act-agreement We note that Canada is still engaged in neogtiations. https://icclr.org/2022/03/29/canadas-future-cloud-act-agreement-with-the-united-states/

[11] https://www.scoop.co.nz/stories/PA2102/S00100/new-zealand-to-join-the-council-of-europe-convention-on-cybercrime.htm

[12] For a full list, see: https://www.digital.govt.nz/standards-and-guidance/technology-and-architecture/cloud-services/about/how/ See also https://www.digital.govt.nz/products-and-services/products-and-services-a-z/

[13] Catalyst was added to the AOG Framework in March 2022. Catalyst has three local data centres in Porirua, Hamilton and Wellington.

[14] https://news.microsoft.com/en-nz/2020/05/06/aotearoa-disclosure/

[15] https://www.datacenterdynamics.com/en/news/hyperscale-data-center-for-new-zealands-south-island-still-on-despite-postponement-of-aluminium-smelter-closure/

[16] https://www.datacenterdynamics.com/en/news/datagrid-acquires-43-hectares-in-south-new-zealand-for-hyperscale-facility/

[17] https://aws.amazon.com/blogs/aws/in-the-works-aws-region-in-new-zealand/

[18] See the Te Mana Raraunga Charter: https://www.temanararaunga.maori.nz/tutohinga

[19] In the National Iwi Chairs Forum (NICF) Mana Ōrite relationship agreements with government agencies, the principle of kaitiakitanga refers to "a shared culture of respect, guardianship, care and protection for data as a strategic and valued resource, recognising that for the NCIF, Māori data is a taonga and iwi-Māori are kaitiaki over their taonga".

[20] CARE stands for Collective benefit, Authority to control, Responsibility and Ethics. See, https://www.gida-global.org/care

[21] https://unesdoc.unesco.org/ark:/48223/pf0000379949

[22] https://development.standards.ieee.org/myproject-web/public/view.html#pardetail/8382

[23] https://www.health.govt.nz/our-work/diseases-and-conditions/covid-19-novel-coronavirus/covid-19-vaccines/covid-19-vaccine-and-your-privacy/covid-immunisation-register-cir-privacy-statement#access-correct

[24] https://www.newsroom.co.nz/challenge-to-bring-home-nz-data-from-overseas-owned-clouds

[25] https://www.newsroom.co.nz/australias-new-encryption-law-threatens-nz-cloud-data

[26] https://stats.govt.nz/about-us/what-we-do/mana-orite-relationship-agreement/

[27] https://data.govt.nz/toolkit/data-governance/maori/

[28] https://shinecollective.co.nz/client-news/data-ilg-enters-mana-orite-agreement-with-department-of-internal-affairs/

[29] https://oag.parliament.nz/2018/public-sector-data/leadership

[30] Infrastructure as a service (IaaS) is a form of cloud computing that provides virtualized computing resources over the internet. https://www.techtarget.com/searchcloudcomputing/definition/Infrastructure-as-a-Service-IaaS

[31] Platform as a service (PaaS) is a cloud computing model where a third-party provider delivers hardware and software tools to users over the internet. Usually, these tools are needed for application development. A PaaS provider hosts the hardware and software on its own infrastructure. https://www.techtarget.com/searchcloudcomputing/definition/Platform-as-a-Service-PaaS

[32] Software as a service (SaaS) is a software distribution model in which a cloud provider hosts applications and makes them available to end users over the internet. https://www.techtarget.com/searchcloudcomputing/definition/Software-as-a-Service

[33] https://www.upguard.com/blog/s3-security-is-flawed-by-design

[34] https://www.upguard.com/breaches/s3-localblox

[35] https://www.upguard.com/breaches/verizon-cloud-leak

[36] https://www.upguard.com/breaches/cloud-leak-chicago-voters

[37] https://businessinsights.bitdefender.com/worst-amazon-breaches

[38] https://www.zdnet.com/article/99-percent-of-all-misconfiguration-in-the-public-cloud-go-unreported/

[39] https://www.zdnet.com/article/elasticsearch-server-exposed-the-personal-data-of-over-57-million-us-citizens/

[40] https://www.pandasecurity.com/en/mediacenter/news/billion-consumers-data-breach-elasticsearch/

[41] https://www.businesswire.com/news/home/20180619005540/en/62-Enterprises-Exposed-Sensitive-Data-Loss-Firebase

[42] There is significant cryptographic research on processing on encrypted data, but we do not think this is yet feasible for the intended applications.

[43] https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report

[44] https://www.aclu.org/issues/national-security/privacy-and-surveillance/warrantless-surveillance-under-section-702-fisa

[45] https://www.legislation.gov.uk/ukpga/2016/25/section/136

[46] https://www.zdnet.com/article/russian-telco-hijacks-internet-traffic-for-google-aws-cloudflare-and-others/

[47] The Department of Internal Affairs website has links to cloud services risk assessments conducted by public service agencies although the actual assessments aren't available on the website. https://snapshot.ict.govt.nz/guidance-and-resources/using-cloud-services/assess-the-risks-of-cloud-services/risk-assessments-completed-by-agencies/index.html

[48] The Department of Prime Minister and Cabinet established the Cyber Security Advisory Commitee in late 2021 and that Committee is due to submit a paper to Cabinet by Q2 2022.

[49] https://www.abc.net.au/news/2020-12-14/google-gmail-youtube-crash-in-massive-outage/12983376

[50] https://www.networkworld.com/article/3648352/top-10-outages-of-2021.html

[51] https://www.submarinecablemap.com/country/newzealand

[52] While the pipe may be interrupted, the data caching process (e.g., AWS Edge) that is used by multinational Cloud providers means that data is or can be replicated or cached in multiple sites around the world at the time of uploading to the Cloud to address latency (also called 'last mile') issues – which in of itself is another challenge for MDSov.

[53] https://www.forbes.com/sites/hisutton/2020/08/19/how-russian-spy-submarines-can-interfere-with-undersea-internet-cables/

[54] https://www.theregister.com/2013/02/07/2e2_data_centre_calamity/

[55] https://www.mbie.govt.nz/science-and-technology/science-and-innovation/funding-information-and-opportunities/process/assessors/

TE KĀHUI RARAUNGA

11/1209 Hinemaru St, Rotorua 3010
admin@kahuiraraunga.io
www.kahuiraraunga.io

Published July 2022