JAMES EVERY-PALMER KC
DPhil (Oxon), LLM (Harv), LLB(Hons), BA(Hons)

By email

Christine Loughnan
General Counsel
Catalyst Cloud
Wellington

21 November 2022

Dear Christine

Te Au Reka and jurisdictional risk

Introduction and summary

1. The Ministry of Justice (**Ministry**) and the judiciary are seeking to procure a new digital integrated case management service for Aotearoa courts and tribunals (Te Au Reka), issuing a Request for Proposal (**RPF**) in October 2022.[1] This is a joint initiative between the executive and judicial branches, involving digitisation of almost all courts and tribunals.

2. The objective is to modernise and simplify engagement with courts and tribunals. Underpinning this project is "the right of all people to access justice and the importance of trust in the integrity of courts and tribunals".[2]

3. Trust is particularly important because our courts and tribunals are the custodians of some of the most sensitive information in the country. A judge or other adjudicator must be fully appraised of all the material necessary to reach a just decision in accordance with the rule of law. While our courts and tribunals seek to be as open and transparent as possible, litigants and witnesses are entitled to expect that confidential material will be accorded appropriate protections whether the material is a State secret, commercially sensitive data, details of a secret witness, or deeply personal information. In addition to confidentiality, the release and use of information is controlled for other reasons, for example, for the protection of a fair trial, to ensure that allegations are not ventilated until they have been tested, and to ensure that information obtained through discovery cannot be used for collateral purposes. Te Au Reka information will also include a judge's notes (including draft judgments) and information about scheduling and other administrative matters.

---

1 Ministry of Justice, *Tāhū o te Ture, Te Au Reka, Request for Proposal*, October 2022 (**Te Au Reka RFP**).

2 Te Au Reka RFP, p 1.

james.everypalmer@stoutstreet.co.nz
D +64 4 915 9271 M +64 275 801 616
F +64 4 472 9029

Stout Street Chambers
6th floor, Huddart Parker Building
No 1 Post Office Square
PO Box 117, Wellington 6140

4. A carefully calibrated set of rules has evolved to determine who can have access to what judicial information and at what time. Some of these rules apply generally,[3] others are in the form of case management directions that deal with the treatment of particular information in a particular case.

5. A key element of Te Au Reka will be ensuring that the storage of court and tribunal files (and associated administrative information[4]) in "the cloud" does not upset the balances struck by these rules. In addition to technical security and availability risks, the introduction of a cross-border element introduces questions as to who can access Te Au Reka information outside of the current processes, under what law and in what circumstances.

6. This issue of jurisdiction risk is addressed by clause 4.5 of the RFP. Vendors are required to meet data sovereignty requirements (including in response to change in the law and the continuing dialogue concerning Māori data sovereignty) and all judicial, court and Ministry information should be located in Aotearoa New Zealand. A potential exception is that information may be permitted to transit or rest in Australia if there is a material benefit from doing so and appropriate processes and safeguards are in place to manage data-related risk and jurisdictional risk.

7. You have sought my opinion as to whether data sovereignty and jurisdictional risks are appropriately dealt with by clause 4.5.

8. In summary, in my view:

   (a) The only way to avoid jurisdictional risk is by holding the Te Au Reka information exclusively in New Zealand and by a provider that is not a subsidiary, or otherwise under the control, of a foreign company.

   (b) As such, in my view, the focus of clause 4.5 is too narrow. Jurisdictional risk also arises where information is held exclusively in New Zealand but by a provider that has a foreign parent company. There are examples of legislation in place overseas which may enable a foreign government to extend its reach to a New Zealand provider through a parent company in

---

[3] See, for example, the Senior Courts (Access to Court Documents) Rules 2017 and the District Court (Access to Court Documents) Rules 2017. The Family Court, the Māori Land Court, Environment Court and Coroners Court have additional or special provisions regarding access to court information. Restrictions apply to certain enactments where the information is likely to be highly sensitive (for example the Adoption Act 1955 or the Care of Children Act 2004). Law enforcement agencies (for example the Police, Serious Fraud Office and Department of Corrections) have access to specified court records as set out in section 173 and Schedule 4 of the Privacy Act 2020. A number of statutes also provide broad rights to certain agencies to search and copy court documents for investigation and law enforcement purposes. Examples include the Inland Revenue Department, Serious Fraud Office, and Security Intelligence Service.

[4] The Te Ake Reka Capability Model provides a summary of the services that will be sought in the RFP and, accordingly, and indication of the information to be held by a provider. A core functionality under the RFP is content management, which involves supporting the management, privacy and access to court and tribunal information. Another is administrative management which requires support of the administrative activities that support the function of courts and tribunal processes. Three further functions are online portals, logistics and procedure management that are more concerned with processes than information.

its jurisdiction. This could occur without notice to the New Zealand government.

(c) I do not regard data held in Australia to be subject to lesser jurisdictional risk than data held overseas generally. Indeed, from the end of this year, data hosted in Australia by an Australian company will be accessible by U.S. law enforcement agencies regardless of whether the provider has a U.S.-based parent company.

(d) The ability to effectively manage jurisdictional risk (for example through holding the data in trust or via New Zealand legislation) is very limited and unlikely to provide sufficient security.

9. I trust that this advice is of assistance, and I would be happy to discuss these issues further.

Data sovereignty and jurisdictional risk

10. Data sovereignty and jurisdictional risk are closely aligned concepts. Data sovereignty is the concept that data remains subject to the laws and governance structure of the country where it is collected.

11. Jurisdictional risk is the risk that an overseas law enforcement agency or other person may be able to obtain lawful access to data stored, processed or transmitted through servers and other infrastructure that are either: (a) located outside New Zealand; or (b) operated by a service provider with a presence outside New Zealand and that may be required to comply with directions by an overseas government or court in relation to that data.[5]

12. The concept of Māori data sovereignty recognises the rights and interests that Māori have in relation to their data, which is considered a tāonga.[6] It refers to the inherent rights and interests that Māori have in relation to the collection, ownership, and application of Māori data.[7] The relevant principles have been articulated in the Te Mana Raraunga - Māori Data Sovereignty Network Charter which emphasises the importance of indigenous data remaining subject to the laws of the nation from which it is collected.[8]

13. The importance of the Crown taking a proactive approach to this issue was identified by the Waitangi Tribunal, explaining:[9]

---

5 Te Au Reka RFP, clause 4.5, p 40, fn3.

6 Te Kāhui Raraunga - the operational arm of the National Iwi Chairs Forum Data Iwi Leaders Group (Data ILG)19 - have defined data as a tāonga.

7 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. The Waitangi Tribunal has recognised that mātauranga Māori includes Māori rights and interests in the digital domain and potential implications for the integrity of the Māori knowledge system.

8 Te Mana Raraunga, *Māori Data Sovereignty Network Charter*. The Charter asserts further that 'Māori Data Sovereignty recognises that Māori data should be subject to Māori governance' and 'Māori Data Sovereignty supports tribal sovereignty and the realisation of Māori and Iwi aspirations'.

9 Waitangi Tribunal, *The comprehensive and progressive agreement for Trans-Pacific Partnership* (Wai 2522), 2021, at p 53.

> We see as particularly problematic the failure to appreciate or understand the link between data and mātauranga Māori, a taonga also guaranteed to Māori under te Tiriti/the Treaty, and in respect of which the Crown has a duty of active protection.

14. Recognising its Te Tiriti obligations, the Government's Strategy for a Digital Public Service includes a commitment to ensure that Māori are involved in decisions relating to digital transformation of the public service.[10] In practical terms, compliance with the concept of Māori data sovereignty means that a vendor will, among other things, need to have processes in place to ensure it has strong controls in place around the usage and sharing of such data, recognising its status as a tāonga.

Information held in a purely domestic cloud

15. As noted in the introduction, the management of Te Au Reka information is a core aspect of the successful operation of our court and tribunals. New Zealand law prescribes how this information can be accessed, by whom, when and for what purposes. Jurisdictional risk opens the possibility that access to this information will also be granted by overseas courts or governments pursuant to their rules around the compulsory provision of information (for example, for law enforcement purposes or between parties engaged in litigation).

16. In the scenario where the information is held on computer servers that are physically located in New Zealand, the information does not transit outside of New Zealand, and the provider is not owned or controlled by a foreign company, no jurisdictional or data sovereignty risks should arise.[11]

17. In other words, the mere fact that the information is in "the cloud" does not make it vulnerable to jurisdictional risk.

International aspects and jurisdictional risks

18. The position becomes more complicated once an international dimension is added to the hosting arrangements.

19. Suppose, for example, that the Te Au Reka information is held in a foreign country by a company that is incorporated in that jurisdiction. Access to the Te Au Reka information could now become exposed to a different set of rules under in the domestic law of that country, including in relation to law enforcement, litigation and regulatory investigations.[12]

---

[10] New Zealand Government, *Rautaki mō tētahi Rāngai Kāwanatanga Matihiko Strategy for a Digital Public Service,* 2020, which sets a whole-of-public-service direction for inclusive digital transformation.

[11] In addition to the contractual arrangements, it may be desirable for legislation to make clear that the information is to be treated as if it was still held by the Ministry, court or tribunal.

[12] This is because any application under foreign law to a foreign court to access the data would not be effective without proceedings in New Zealand. A New Zealand court would apply New Zealand law to an application under (for example) the Senior Courts (Access to Court Documents) Rules 2017, and it is difficult to see in what circumstances an application to access court documents pursuant to some other cause of action could be governed by foreign law: see generally Maria Hook & Jack Wass *Conflict of Laws in New Zealand* (LexisNexis, 2020) at 301-303.

20. It is difficult to imagine how this second set of access rules could be avoided in this scenario. Any contractual restrictions on access to the information would be trumped by the host country's laws.[13] Even if the New Zealand Parliament passed legislation purporting to prevent access under the host country's domestic laws it is very unlikely that this would be given effect to as a matter of private international law.[14]

21. These risks are recognised by the RFP and are the basis for clause 4.5.

22. However, clause 4.5 makes two implicit assumptions about the nature of jurisdictional risk which, in my view, are very questionable.

Clause 4.5 wrongly assumes that jurisdictional risk only arises where data leaves New Zealand

23. First, clause 4.5 assumes that jurisdictional risk only arise when the information in question is located (at rest or in transit) outside of New Zealand.

24. However, in my view, where the information is held exclusively in New Zealand by a New Zealand company, jurisdictional risk still arises where the provider has an overseas parent. In this scenario, the parent's home country may assert jurisdiction over data that an entity holds or has control of in Aotearoa New Zealand. So, for example, the home jurisdiction of the parent may provide for discovery of information that is within the possession or control of the parent even though it is held by a subsidiary in New Zealand.[15]

25. A topical example of the home jurisdiction of the parent asserting extraterritorial jurisdiction over data held by subsidiaries around the world is the Clarifying Lawful Overseas Use of Data Act (United States) enacted in 2018 (**CLOUD Act**) which allows U.S. federal law enforcement to compel U.S.-based technology companies[16] to disclose data pursuant to warrant[17] regardless of where it is located.[18] The test for application of the CLOUD Act to data outside the US is

---

[13] The foreign court would have personal jurisdiction over the custodian, and arguably subject-matter jurisdiction given that the data was held there. An application for discovery in relation to court proceedings, for example, is a matter of procedure that would governed by the law of the foreign country, even if the data related to proceedings in New Zealand: see Hook & Wass at [3.145].

[14] For example, the court may (i) decide that the matter is not contractual, so any contractual restrictions do not apply, (ii) find that the contractual restrictions are not binding on the party seeking access to the information, or (iii) characterise its own access rules as overriding mandatory rules that apply regardless of what the applicable law provides: Hook & Wass at 278-291.

[15] See ibid. Under New Zealand law a person cannot generally object to production of relevant documents on the basis that the place where the data is held would prohibit production: *Brannigan v Davison* [1997] 1 NZLR 140 (PC). This will depend on the interpretation of the laws of the parent's home country and whether they are intended to have extraterritorial or overriding effect.

[16] Being companies that provide electronic communication or remote computing services. The CLOUD Act applies to warrants.

[17] The CLOUD Act (by way of the Stored Communications Act (codified at 18 USC Chapter 121 §§ 2701–2712)) applies to warrants issued using the procedures described in the Federal Rules of Criminal Procedure (and equivalent procedures in the case of a State court or a court-marshall). See USC § 2703(a)

[18] CLOUD Act section 103, amending the USC adding § 2713: A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or

that the data is within the US provider's "possession, custody or control". Where this test is met, U.S. jurisdiction is treated as applying to the off-shore data, without raising issues of comity.[19] There is no requirement for notice to the entity whose customer or subscriber data is being sought or to the foreign government.[20] This extraterritorial legislation has been subject to considerable academic criticism.[21]

26. A second example from the U.S. is the Foreign Intelligence Surveillance Act (**FISA**)[22] which enables U.S. intelligence agencies to require cloud hosts to provide data they control, store, or manage, as well as encryption keys to decrypt that data relating to non-U.S. persons. While it does not have explicit extraterritorial reach, if the U.S. providers have the ability to remotely access servers hosted outside the US or to require subsidiaries to provide access, then the data stored there can be seized. FISA requests tend to be secret and do not require a warrant.

27. Another form of jurisdictional risk is where the parent company is compelled to provide information or documents through the parent country's rules of civil procedure (that is, discovery) or where a regulator in the parent country exercises compulsory information gathering powers. Information held by a New Zealand subsidiary which comes within the request may have to be provided as being within the control of the parent company.

28. Data trusts have been mooted as a model that might insulate a subsidiary against the extraterritorial jurisdiction of the parent country. This model posits a trustee managing the collection and use of data and controlling the encryption keys so that the data is not under the control of either the provider company or its foreign parent. However, I understand that this is not feasible in practice as the services

---

other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States.

19 A key purpose of the CLOUD Act was to address barriers arising from the mutual assistance process that usually applies to the enforcement of law enforcement warrants between countries by enabling direct enforcement as if the data was subject to US jurisdiction. See, for example, sec 102 of the CLOUD Act, which sets out the Congressional Findings.

20 Under the Stored Communications Act 18 USC § 2703, disclosure pursuant to a warrant can be required without notice to the customer or subscriber notwithstanding the provider is not authorised to access contents other than for providing the storage of computer services USC § 2703(b). Under the CLOUD Act, the US provider is permitted (although not required) to give notice to an entity within the foreign country whose customer or subscriber information is being sought, where the customer or subscriber is a national of the foreign country. However, this only applies for a qualifying country, being one that has CLOUD Act agreement with the US. Such notice is permitted but not mandatory and the express permission suggests it may be unlawful to give notice in other circumstances.

21 See for example Sabrina A. Morris "Rethinking the extraterritorial scope of the United States' access to data stored by the third party" (2018) 42 Fordham Int'l L., J, 183, which identifies problematic aspects of the CLOUD Act and recommends amendments; Secil Bilgic "Something old, something new, and something moot: the privacy crisis under the CLOUD Act" (2018) 32 Harv.J.L. & Tech. 321 at 347 which opines that post-Snowden attempts by US technology companies to find ways to ensure data privacy abroad, for example by Microsoft created a data trustee system and others signed privacy contracts with foreign customers, were rendered moot by the CLOUD Act and concludes '[r]egardless of where data is located, as long as a US-based company [has possession, custody, or control] the US government will be able to access it'.

22 Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 (FISA), 50 United States Code [USC] § 1881a.

required for Te Au Reka, as outlined in the capability requirements,[23] will require the provider to have access to decrypted data. The only way to achieve data opacity is for the customer (the Ministry and judiciary) to only transfer encrypted data to the cloud provider and hold its own encryption keys. This, however, means that the applications must be run within the customer's own computing environment which defeats the purpose of moving to a cloud provider.[24]

29. As summarised in Te Kāhui Raraunga *Māori data sovereignty and offshoring Māori data* (July 2022, at p 11):

> 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.

Clause 4.5 wrongly assumes that jurisdictional risk in relation to Australia is manageable

30. Secondly, clause 4.5 assumes that jurisdictional issues are lesser in Australia than in other countries and can be managed. This is the basis for the potential exception to data remaining in New Zealand.

31. In my view, this assumption is also not correct.

32. Where the server is located in Australia, it will be subject to Australian access rules in terms of law enforcement and the compulsory provision of information in litigation and pursuant to powers of regulators.[25] As discussed at paragraph 19 above, it is unlikely that New Zealand legislation which tried to prevent this outcome would be effective.

33. As well as Australia asserting jurisdiction over the data, there is also the risk of a third country accessing the information.

34. Again, the CLOUD Act is instructive. In addition to its base provisions, the CLOUD Act provides for bilateral CLOUD Act Agreements to be negotiated. Once in place, these agreements will enable law enforcement agencies in the U.S. to obtain access to electronic data held by providers in the other country whether or not the provider has a U.S.-based parent company. The Australia-US CLOUD Act Agreement was signed in December 2021 and anticipated to come into force at the end of 2022.[26]

---

[23] See note 4 above.

[24] In this scenario, I note that the data is still vulnerable to a "harvest now decrypt later" attack where Te Au Reka information is obtained now and decoded in the future as decryption technologies develop.

[25] See paragraph 19 above.

[26] Agreement between the Government of Australia and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime, Australia-United States (Signed 15 December 2021). It is given effect to by the Telecommunications Legislation Amendment (International Production Orders) Act 2021.

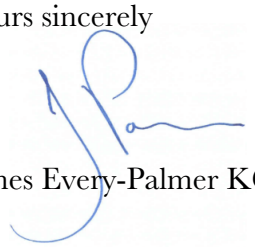
35. What this means is that in addition to having access to data held by an Australian company with a U.S. parent, from the end of 2022 U.S. law enforcement agencies will be able to utilise the Australia-US CLOUD Act Agreement to access data in Australia held by an Australian company *even where there is no US parent company*. That is, the Agreement enables direct enforcement of disclosure orders against providers in Australia irrespective of any US connection. In the context of the Te Au Reka RFP, if the data is possessed or controlled by a provider incorporated in Australia (including through a subsidiary in Aotearoa New Zealand), the information is subject to the Australia-US CLOUD Act Agreement. Similar to the broader operation of the CLOUD Act explained above, there is no requirement in the Australia-US CLOUD Act Agreement to provide notice to the Australian government or the entity whose customer data is being sought.[27]

Conclusion

36. In my view, Te Au Reka information will be subject to jurisdictional risk where the cloud provider has an offshore parent and/or where the data transits or rests in any foreign country (including Australia). I have referred to the CLOUD Act as a topical example. But, the risk is broader than the CLOUD Act as it arises wherever a foreign country may assert jurisdiction over the Te Au Reka information through a foreign parent or because the data is located in that foreign country. Future laws may also be more invasive than the CLOUD Act.

37. Accordingly, there is a material risk in relation to the court files and administrative information held overseas or in New Zealand by the provider with an overseas parent. The risk is problematic in terms of trust in the judiciary and is particularly problematic for Māori data sovereignty. In my view, it is very difficult to see how such risks could be managed effectively. I also note that, in relation to servers located overseas, it would be very difficult to provide for government oversight of key infrastructure in a way that oversight occurs in relation to telecommunications networks under the Telecommunications (Interception Capability and Security) Act 2013.

Yours sincerely



James Every-Palmer KC

---

[27] Australia-US CLOUD Act Agreement. sets out various "protections", but other than protections against targeting individuals among other things, these are limited to simply agreeing to apply the domestic law of the issuing authority (see for example Article 3, clause 4). The CLOUD Act also allows for a court to modify or quash a legal process where the following conditions are met: the disclosure would cause the provider to violate the laws of the qualifying foreign government; the interests of justice dictate that the legal process should be modified or quashed; and the customer or subscriber is not a US person and does not reside in the US. Of concern, these conditions indicate that, as a starting point, the warrant could be inconsistent with the law of the receiving country and apply to data of a non-US person. The requirement that the warrant would cause the provider to violate the laws of the qualifying foreign government also requires a law that specifically prohibits compliance (which many countries do not have). The "interests of justice" criterion also provides the US courts with a broad discretion as to whether to modify or quash.