National Cyber Security Centre

GUIDANCE

The NCSC is part of the Government Communications Security Bureau

July 2019

FAQs: Lawful access to official data offshore

The National Cyber Security Centre (NCSC) has prepared the following guidance to provide agencies with high-level information about lawful access to official data held in jurisdictions outside of New Zealand.

Introduction

Any official data stored or managed offshore (outside of New Zealand) is subject to the laws of the jurisdiction where the data is geolocated. This means that foreign governments may be able to gain access to New Zealand Government data under the justification of "lawful access" without the knowledge or consent of the data owner.

Q: What does "lawful access" mean?

A: Lawful access is an investigation technique used by national security and law enforcement agencies. It entails the interception of private communications and the seizure of information where authorized by law.[1]

More simply, lawful access can be described as access to data by a government where that access is granted under the provisions of official legislation.

[1] https://hillnotes.ca/2014/10/21/lawful-access-and-privacy-the-legislative-framework/

Q: What types of legislation could be used to justify lawful access?

A: Lawful access to data may be granted under a wide range of laws and legislation. Some will be obvious, such as law enforcement, state surveillance and national security legislation, while others might be more obscure and therefore harder to identify.

Legislation regarding 'national security' and 'national interests' may be used by foreign governments to justify state access to data held within their jurisdiction, with a low threshold.

Q: What is the threshold for lawful access?

A: The threshold for accessing data lawfully will vary greatly between jurisdictions, depending on the provisions and authority granted under their national security or law enforcement legislation.

In some jurisdictions, the state must have adequate reason to believe that there is a threat to national security (and can evidence these concerns) before accessing private data. In many jurisdictions, the state may access data under the proviso of national security with little or no evidence. In a few jurisdictions, the state can access private data without any evidence or justification.

When assessing the jurisdictional risk associated with locating New Zealand Government data offshore, it is important to consider the threshold for lawful access set out in the legislation of the jurisdiction. However, it is important to remember that

- foreign jurisdictions are under no obligation to notify New Zealand Government agencies of legislative changes that might affect lawful access to data held in their jurisdiction
- legislation can change quickly, without your knowledge
- it may be challenging and onerous to routinely monitor legislative changes in foreign jurisdictions

Q: Does a foreign government have to seek permission before lawfully accessing official data?

A: In many cases, legislation (national security laws in particular) enables foreign governments to access data without the permission or knowledge of the data owner. Some foreign governments may notify New Zealand Government agencies of their intention to access official data, however in most instances, foreign governments are under no obligation to do so before or after gaining lawful access to official data.

https://www.ncsc.govt.nz

Q: Will my cloud service provider notify me when my data is accessed lawfully?

A: Not necessarily - in some jurisdictions, national security legislation allows the state to issue the service provider with a 'gag' order, preventing the service provider from notifying the data owner that their information has been accessed without their authority.

It is noted that some service providers make significant effort to ensure the data owner is notified when lawful access occurs, however this can be overridden in most cases by the legislation used to justify lawful access within the jurisdiction. Even if your service level agreement (SLA) requires your service provider to notify you when your data is accessed, the gag order will likely override the provisions of the SLA.

Q: How do I know where my data is stored and managed?

A: The exact geolocation of your data should be clarified with your cloud service provider including the primary location of your data and the location of any backup data repositories held in other jurisdictions.

It is very possible that your data may be geolocated in a low risk jurisdiction most of the time, but the backup data center is located in a high-risk jurisdiction. Managing data over multiple jurisdictions is complex, making it difficult for agencies to accurately assess the risks associated with locating data offshore. Agencies should consider requirements for the location of primary and backup servers equally when assessing the suitability of the jurisdiction and the service provider for handling official data.

Q: Can I specify a geolocation in the SLA with my cloud service provider?

A: In most cases, yes. The NCSC strongly encourages agencies to undertake a robust risk assessment and identify which jurisdiction is the lowest risk for storing and managing official data offshore. Once you have identified your preferred jurisdiction, the geolocation can be specified in the SLA with your cloud service provider (where possible).