BUDDLE FINDLAY

CLOUD Act – Law enforcement access to cloud data

Allan Yeoman, Amy Ryburn, Philip Wood, Damien Steel-Baker, Keri Johansson, Renee Stiles

15 May 2018

In March we reported on the issue regarding the ability of United States (US) law enforcement to access your cloud-based data, regardless of the country in which it is stored. That issue was to be considered by the US Supreme Court in *Microsoft vs the United States of America*. Since the Supreme Court heard the case but before it released its judgment, the US Congress has passed the Clarifying Overseas Use of Data Act (CLOUD Act). This legislation clarifies law enforcement agencies' rights to access your data and renders the Supreme Court decision unnecessary. The Supreme Court has now ordered that the case be dismissed.

CLOUD Act

The CLOUD Act amends the Stored Communications Act to clarify the data that US and foreign law enforcement agencies can obtain from US-based providers of electronic communication services or remote computing services, such as cloud services.

US law enforcement can compel, through a warrant or similar process, access to data that is within the provider's "possession, custody, or control" and regardless of whether such data is "within or outside of the United States."

A provider can apply to modify or quash the warrant if it reasonably believes that:

- The subject of the request is a non-US person who resides outside the US
- Complying would create a material risk that the provider would violate the laws of a "qualifying foreign government". A qualifying foreign government is a government that has entered into an executive agreement with the US government (more below).

If a provider makes an application to modify or refuse a request for data, the court will conduct a conflict of laws analysis to determine whether the provider should be required to provide the data. The CLOUD Act also preserves common law comity claims (a conflict of laws doctrine) as an option for countries that have not entered into an executive agreement, although that option remains untested.

The CLOUD Act also enables law enforcement agencies from other countries to request data stored by US providers if the request:

- Does not target US persons or persons located in the US
- Comes from a country that has an executive agreement with the US.

No executive agreements exist yet. Over time executive agreements will be entered into between the US government and governments of other countries to enable cross-border access to data. Each agreement must be presented to Congress with certification from the US Attorney-General that the relevant government satisfies the standards set out in the CLOUD Act. These standards include "robust substantive and procedural protections for privacy and civil liberties". The CLOUD Act provides further detail regarding what these procedures must include, such as orders for the production of information must be subject to the review of a court or other independent authority in the relevant country.

Several large cloud providers supported the CLOUD Act, including Apple, Google, Facebook and Microsoft. These providers signed a joint letter to Congress that stated "if enacted, the CLOUD Act would be notable progress to protect consumers' rights and would reduce conflicts of law."

However, the CLOUD Act provides US law enforcement potentially broad access to data stored in the US and abroad. Foreign law enforcement agencies now also have a potentially easier way to request information directly from providers under an executive agreement, rather than using other government-to-government channels. These rights have been criticised by privacy advocates as an unnecessary expansion of investigative powers.

Relevance to New Zealand

As noted above, US-based cloud service providers can resist US law enforcement access to New Zealand residents' data on the

basis that it is information about a non-US person who resides outside the US. However, to challenge access on that basis (without relying on common law comity grounds):

- There must be an executive agreement between the US and New Zealand or the country in which the data is stored. We understand that the first executive agreement is likely to be between the US and UK but have no information about when this may come into force or any possible agreement with New Zealand
- The provider to which the request is made must file potentially costly court proceedings to modify or quash the request
- The court must find a conflict of laws and that the "interests of justice dictate" that the order granting access to the information should be modified or quashed.

New Zealanders will therefore rely heavily on service providers to resist requests for their data.

Until executive agreements are in place it appears there are only limited, and untested, common law comity grounds available to resist orders for access to information. Given this, it seems likely that, if presented with a valid warrant covering New Zealanders' information, a US-based cloud provider would give access to that information. New Zealanders entering into contracts with such providers may want to consider seeking contractual obligations on providers to file proceedings resisting access to data where possible.

Auckland

188 Quay Street
Auckland 1010

PO Box 1433
Auckland 1140
New Zealand

P: +64 9 358 2555
F: +64 9 358 2055

Wellington

Aon Centre
1 Willis Street
Wellington 6011

PO Box 2694
Wellington 6140
New Zealand

P: +64 4 499 4242
F: +64 4 499 4141

Christchurch

83 Victoria Street
Christchurch 8013

PO Box 322
Christchurch 8140
New Zealand

P: +64 3 379 1747
F: +64 3 379 5659