BUDDLEFINDLAY

Microsoft vs the United States of America - law enforcement access to cloud data

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

21 March 2018

In 2018 the United States (US) Supreme Court will consider an important case regarding law enforcement's ability to access information stored in the cloud. This case will help determine the extent to which US law enforcement agencies may be able to access your data, regardless of what country it is stored in.

Case history

The case began in 2013, when Microsoft was issued a search warrant requiring it to provide content from an email account that was thought to be linked to drug trafficking. In response to the warrant, Microsoft provided information about the account itself, which was stored in the US, but refused to turn over email content that was stored in Ireland (although accessible from the US).

A federal magistrate ordered Microsoft to provide the content stored in Ireland. Microsoft appealed, and in July 2016 the court of the Second Circuit overturned the ruling and invalidated the warrant. In January 2017 the full court of the Second Circuit split 4-4 on an application to rehear the case, leaving in place the judgment that Microsoft does not have to provide the information stored in Ireland.

This left the government with only the ability to request the information from Irish authorities under an international treaty process, which is generally more difficult and time-consuming. The government appealed and the Supreme Court heard the case in late February 2018. The Supreme Court is expected to release its judgment prior to the summer recess in June 2018.

Since the Second Circuit's ruling invalidating the warrant issued to Microsoft, Google has been involved in similar litigation – with the opposite result. At least four magistrate judges in four states (Pennsylvania, Florida, Wisconsin, and California) have ordered Google to comply with search warrants in respect of email content that is accessible from the US.

This means that the outcome of the Supreme Court case will be keenly watched by a number of interested parties.

Key location – data, user and requestor

The Microsoft case focused on the location the data is stored (Ireland). The more recent cases involving Google considered that the key issue is the location where the search warrant is executed in, and therefore where the information is accessed from. The location of the user has played no part in the Microsoft case and his or her nationality and residency has never been revealed.

It can be argued that the Microsoft decision leads to a bizarre outcome, which the court itself recognised. It could mean that for a crime committed in the US by a US resident using services provided by a US company, with the only international component being a business decision to store data abroad, law enforcement may have considerable difficulty obtaining critical evidence.

There is debate about whether the physical disconnect between the location of users and their data is significant. Google's general counsel Kent Walker has said in a speech that "law enforcement requests for digital evidence should be based on the location and nationality of users, not the location of data." Regardless of whether or not you agree, this position would be difficult to achieve internationally due to the potential conflict of laws between the jurisdictions of the user, the requestor, and the data.

One reason Ireland is often chosen as a location for data storage is because it is subject to the European General Data Protection Regulation (GDPR). If the Supreme Court upholds the government's warrant, Microsoft's compliance with the warrant in the US could potentially put it in breach of its obligations in Ireland under the GDPR.

Information stored in the cloud is different to physical evidence. For physical evidence, the location of the evidence is more important as it must be physically taken from that place. In contrast, data stored in the cloud is generally accessible by the click of a button. Although court cases indicate that Microsoft and Google restrict the extent to which their personnel in the US can access offshore data, it does appear from their submissions that it is possible to access it from the US without input

from the foreign jurisdiction. Microsoft's online service terms also allow Microsoft to transfer data to the US at any time, regardless of where the data is stored.

The way in which Microsoft and Google store data also appears to be different and may impact the relative importance a court would place on the location of the data and the location of the user. Microsoft was clear that the emails requested were stored on a server in its Irish data centre. Google submitted in its cases that its user data is stored in packets that may be located in different data centres across the world and that such data is not stored, at least for any appreciable period, in a single identifiable location. While in the Microsoft case, the government has a second option to access data via international treaty processes, that option may not be possible for Google's data.

Whether or not the Supreme Court considers the location of the user is important may have an impact on the ability of US law enforcement to access data about residents of other countries (including New Zealand), regardless of where the information is stored. It could also impact the precedent value of the case across multiple suppliers and storage methods. If the court focuses only on the location of the data, it may be difficult to determine what the position is for a company like Google, which does not store data in an identifiable location.

The US currently has a bill before the Senate (the International Communications Privacy Bill), which aims to reform law enforcement access to information to better reflect cloud computing. This Bill focuses on the location of users rather than data by drawing a distinction between "US persons" and foreigners. In the event that the Bill is passed, it may overtake the Supreme Court decision in the future.

Frequency of US law enforcement requests

The Microsoft and Google cases have all involved warrants under the Stored Communications Act 1986 (SCA). This US legislation relates to general law enforcement, such as the suspected drug trafficking in the Microsoft case. Quite separately, US legislation such as the Foreign Intelligence Surveillance Act 1978 (FISA) and the USA PATRIOT Act (the Patriot Act) enables collection of information in respect of suspected espionage or terrorism. The Supreme Court decision will have no impact on access to information under FISA or the Patriot Act.

Google releases statistics about law enforcement requests made to it. The most recent full year available is to the end of June 2017, which shows 157,419 requests for users' content (eg content of emails) and 94,491 requests for user data (eg information about an account). Google discloses data in response to approximately 60-65% of those requests.

Requests to Google under FISA (ie in relation to suspected espionage or terrorism) are not reported in as much detail, but Google has said that in the six month period from January 2016 to June 2016 it received between 500-999 requests for email content about 25,000–25,499 users, and in the six month period from July 2016 to December 2016 it received 500-999 requests about 35,000–35,499 users (these are the most recently reported periods). There is no reporting on Patriot Act requests.

This is a substantial number of requests, totalling several hundred per day, and this is only one provider. The outcome of the Microsoft case therefore has the potential to impact many users internationally, including in New Zealand, as we explain below.

Relevance to New Zealand

With US-based companies such as Microsoft, Google, and Amazon currently providing the bulk of public cloud services, the outcome may impact many New Zealanders whose data is held by those suppliers. It will also impact the New Zealand subsidiaries of US companies in relation to the data they store in New Zealand. The potential reach of the case was recognised by our Privacy Commissioner, who submitted a brief to the Supreme Court in December 2017.

New Zealanders' information is also often stored in data centres in Sydney, Singapore or Ireland when using services provided by US-based companies. Some services include an ability to specify which data centre or region will store your information. Many customers use this option to ensure data is stored outside the US due to concerns over US privacy laws and the rights of access for law enforcement and surveillance. This case may impact on how effective exercising that option is. We will report on the Supreme Court decision when it becomes available later in the year.

This article was updated after it was first published as the Supreme Court heard the case between writing the article and publication. The original version stated that the court was expected to hear the case before June 2018.

Auckland

PwC Tower
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