

The Cloud and US Cross-Border Risks

By Connie Carnabuci and Heather Tropman

Connie Carnabuci is a partner at Freshfields Buuckhaus Deringer, in Hong Kong and Head of the IT practice group, and is an international expert on cloud computing legal issues. Connie has 25 Years IT legal practice experience. Connie was previously a partner at Mallesons Stephen Jaques in Sydney.

Heather Tropman is the General Counsel at Macquarie Telecom and has over 13 years of legal experience in both private practice and in-house with a focus on IT and IP. Heather held previous roles at Aristocrat Technologies (Global IP Counsel), Gilbert and Tobin Lawyers (Senior Associate) and Olser, Hoskin & Harcourt Lawyer (Canada)

This paper analyses the key risks associated with storing data in the U.S. to assist Australian businesses and government in taking a holistic, balanced and informed view of their data storage options.

The opportunities presented by improved global networks and the internet have allowed some hosting service providers to offer Australian customers data storage in offshore jurisdictions through global or regional Clouds.

As many of the commercially available Cloud computing services are in the U.S., this analysis compares Australian and U.S. laws and regulations to identify the relative advantages of storing your data in Australia.

While the potential cost benefit of shifting data storage overseas (or within a global Cloud) may appear simple to calculate, the risks of managing compliance and navigating the cross-border legal landscape are hidden costs not often considered in the business case.

Data is subject to the laws of the jurisdiction in which it is stored. For Australian customers considering a move to offshore data storage in the U.S., this has potentially wide ranging implications.

Can your data be sent offshore?

The first step in considering whether to store your data offshore is to confirm whether the data relating to a particular business activity or the particular type of data involved can readily be sent offshore, from a regulatory and compliance perspective.

Any regulated entity and businesses using or storing personal or business sensitive data should exercise particular caution. For example, the Australian

Prudential Regulatory Authority (APRA) which oversees the domestic financial services sector, has stated that financial services companies that wish to transfer data offshore must first notify APRA and demonstrate to the regulator that appropriate risk management procedures are in place to protect the data. The company must also secure guarantees in its contract with the data hosting company that APRA will have access to that company to conduct site visits if required. In the context of the global Cloud, where the third party provider is likely to be using one of a number of data centres in different countries, this has proved to be a difficult issue to overcome because providers have been reluctant to provide guarantees around data security to a level which is satisfactory to the regulator. APRA's approach to date has been cautious.

Some classes of customer may simply refuse to have their data transmitted and stored overseas. For example, the Commonwealth of Australia Government Contract for IT Services expressly prohibits suppliers from transmitting or storing their customer data outside of Australia.

How do you effectively maintain compliance across multiple jurisdictions?

Data stored in an offshore Cloud may move across multiple foreign jurisdictions, each with its own set of rules. As such Australian based customers would have limited visibility over where their data is at any point in time, seriously reducing their ability to ensure continuing regulatory compliance with Australian law and to manage the associated non-compliance risks. Imposing strict compliance reporting or audit provisions in your Cloud service agreements will have cost and price implications. However, U.S. Cloud service

agreements are typically on standard “click wrap” terms. In any event, the value of any audit right (if obtained) is also questionable given that the results only verify the state of the data at the particular time of the audit and it is difficult (if not impossible) to constantly supervise the data considering the virtual nature of the Cloud.

In Australia, there is concern regarding compliance with Payment Card Industry Data Security Standards in a global Cloud. Those standards include requirements such as restricted physical access and the ability to track and monitor all access to card details. Community concern around data privacy is also rising, leading to greater regulator scrutiny and many companies are concerned that storing their data in an offshore Cloud will jeopardise their ability to continue to adhere to the National Privacy Principles. This is particularly so in light of the Australian Government’s Exposure Draft which, if enacted, will introduce even more stringent regulation of cross-border disclosures of personal information. Under the Exposure Draft, if a company holding “personal information” in Australia discloses that information to an offshore recipient, it may be vicariously liable for any misuse of that personal information by its offshore Cloud provider.

A lack of consistency in privacy laws across jurisdictions makes monitoring continuing compliance with Australian law and assessing risk of non-compliance extremely difficult and expensive. Unlike Australia, the U.S. does not have a comprehensive overarching data privacy regime and has taken a sector specific approach by enacting laws only when required by specific industries or circumstances. The upshot is that there has been very limited take-up of offshore Cloud-storage (PaaS or IaaS) opportunities among Australian companies, particularly those businesses that rely on a high level of data privacy protection and security.

In an effort to address some of these concerns, some commentators (such as Microsoft) are calling for a “free trade” type agreement, which effectively sets up bi-lateral agreements between governments for adherence to a universal set of operational standards in respect of the Cloud. Whilst universal standards would help remove operational uncertainty, they are likely to result in additional “compliance” costs to service providers which would be automatically passed on, unless there is an agreed change control provision in the contract (which is unlikely under standard terms).

What are the tax consequences of hosting a transactional website in the US and the resultant data collection?

Hosting a transactional website on servers in the U.S. can create a taxable presence for U.S. federal income tax purposes. While mere storage of data typically should not amount to the conduct of business within the U.S. for tax purposes, the activity can be treated as the conduct of business if the non-U.S. person stores data for the

account of others, or allows customers or other third parties access to the data.

If a website within the U.S. does involve the conduct of business, an Australian company entitled to the benefits of the Australian-U.S. income tax treaty might have a taxable U.S. presence if the website arrangements constitute a permanent establishment. Website arrangements could constitute a permanent establishment of the company if:

- (i) the company contracts for the right to use particular facilities such as a particular data center within the U.S.;
- (ii) the company’s requirements mandate its exclusive use of particular facilities; or
- (iii) the facilities provider is not a legally and economically independent third party providing the facilities in the ordinary course of its business of providing similar services to many other unrelated customers.

Whether a particular website arrangement would create a taxable presence for U.S. federal income tax purposes would need to be evaluated in light of all of the facts (principally, the terms of the arrangement, the transactional activity and the circumstances of the storage provider).

Any non-U.S. person that conducts business within the U.S. must file a U.S. income tax return even if the person does not have a U.S. permanent establishment. There are penalties for failure to file, even if no tax is due. Such penalties may prove especially problematic for Australian entities with future plans for future expansion into the U.S.

Once a particular U.S. service or facilities provider or location has been identified, U.S. state and local taxes also need to be considered. Most U.S. states and some U.S. localities impose income tax, which sometimes can apply to non-U.S. persons that are not subject to U.S. federal income tax. Some states (such as California) may tax an allocable part of the non-U.S. income earned by a global business doing business within their borders. States and localities also impose business and licensing taxes, and they may apply to a non-U.S. person doing business within the jurisdiction even if that person has no computer or other facilities within the jurisdiction.

It is important to note that U.S. states and localities impose sales taxes on sales of goods (and sometimes sales of services) made within their jurisdiction. Sellers generally are liable to collect and remit those taxes. States and localities increasingly have asserted that e-commerce sellers operating outside their borders who regularly make sales to persons within their borders may be liable to collect sales tax.

U.S. TREASURY RULES OBLIGE THE AUTHORS TO TELL YOU THAT STATEMENTS ABOUT U.S. TAX MATTERS IN THIS PAPER ARE GENERAL

AND PRELIMINARY ADVICE ON WHICH YOU CANNOT RELY TO AVOID U.S. TAX PENALTIES.

Will storing your data offshore subject you to the jurisdiction of the US courts?

Data stored in the U.S. is subject to U.S. law, regardless of whether the data user or the data subject is based in Australia, or elsewhere.

However, whether the receipt or transmission of data over the Internet on a server located in the US is sufficient for a US court to assert that it has jurisdiction over the parties is an area of U.S. law which is far from settled.

Generally speaking, whether a U.S. court may assert personal jurisdiction over a non-resident defendant turns on whether an exercise of jurisdiction comports with the requirements of the Due Process Clause of the U.S. Constitution. The touchstone of this analysis is whether the "defendant purposefully established "minimum contacts" in the forum state".¹ The minimum contacts requirement is premised on the notion of purposeful availment, which ensures that a non-resident defendant will not be hauled into court based upon "random, fortuitous or attenuated" contacts with the forum state.² In short, a non-resident defendant's contacts with a jurisdiction must have a basis in "some act by which the defendant purposefully avails itself of the privilege of conducting activities within the forum state".³ In most Internet contexts, advertising alone is an insufficient basis for exercising personal jurisdiction over a non-resident defendant who has no active contacts with the forum state. To be hauled to court in the forum, the non-resident defendant generally must have had systematic and continuous contacts with the state, as demonstrated for example by the number of internet sales to the forum residents, the volume of business generated in the forum and the amount of revenue earned from sales with residents of the state.

Today, the long-standing principles of personal jurisdiction in the U.S. face serious challenges stemming from the rapid advancement of electronic telecommunication services and offshore data sharing and storage worldwide. Faced with a borderless communication medium, U.S. courts have been increasingly inconsistent in their interpretation and application of the minimum contacts test and their assertion of personal jurisdiction in the internet context.

Some courts have asserted jurisdiction in civil tort and criminal cases where the data transmission comprises part of the crime or intentional tort, or where there is evidence that a party specifically or intentionally directed a data transmission to the jurisdiction. Some states have enacted aggressive jurisdictional statutes which permit the exercise of personal jurisdiction over non-residents who use a computer (or computer network) located within the state, limited only by vague

notions of fairness embodied in the U.S. constitution. At the same time, where a party transmitting the data to a remote database was not aware that the subject database was located within the jurisdiction, courts have held that the mere act of accessing a computer database remotely is an insufficient rationale for asserting jurisdiction.

In addition, if you enter into an agreement with a U.S.-based Cloud provider for the use of servers located in the U.S., in the absence of clear contractual language to the contrary, a U.S. Court would likely find that it had jurisdiction over any issue or dispute arising out of, or in connection with, that agreement. In most cases, contracts with offshore global Cloud providers contain a foreign governing law and submission to foreign jurisdiction and it would be prudent to seek foreign legal advice in relation to both the interpretation and the enforcement of the contract.

Litigating anywhere offshore is more costly and inconvenient for a business located in Australia. However, due to the breadth and reach of U.S. discovery laws, the costs of litigation in the U.S. in particular, are typically far greater than in Australia.

What document retention obligations does the offshore location impose on you?

If you do fall within the jurisdiction of the US courts then you will also need to ensure you can comply with the civil procedure rules regarding retention and discovery of documents. For example, U.S. Rule 34 of the U.S. *Federal Rules of Civil Procedure* imposes a legal duty on companies to retain all documents, including electronic documents, that may be relevant to pending and reasonably foreseeable litigation. During the discovery process, companies with data stored in the U.S. could be required to produce this data. It is possible that storing data within the U.S. may provide enough of a connection for a U.S. court to find jurisdiction over an Australian company storing its data there and subject the company to the US discovery obligations.

In comparison, Australian civil procedure rules regarding discovery and document retention are less onerous.

Will you be able to effectively enforce your rights against a foreign Cloud provider and what remedies are available to you?

It would be extremely difficult to enforce a statutory right arising under Australian law in the U.S., as those laws would not necessarily have extraterritorial effect. Even if a contract with a U.S. Cloud provider is governed by Australian law (which is unlikely under standard terms), enforcement of that contract in a U.S. Court will require expert evidence as to the interpretation and effect of the Australian law, which is costly and difficult.

A U.S.-based Cloud provider would be required to comply with U.S. laws and obey all orders issued by a

U.S. Court, even if compliance caused the provider to violate an order issued by an Australian Court.

Even where there is no conflict between U.S. and Australian law, a U.S. court is not obligated to automatically give effect to the orders of an Australian court, absent a specific treaty or U.S. legislative rule. The U.S. is not a party to any treaty for the mandatory enforcement or recognition of foreign judgments. Thus, for a U.S. court to give effect to an Australian judgment, it must be justified under general principles of comity, i.e., it would have to be shown that the U.S.-based Cloud provider was subject to Australian law and had been given adequate notice and an opportunity to be heard by the Australian court, and that the Australian order did not offend the public policy of the U.S. forum state.

Further, an Australian court is likely to be reluctant to exercise its discretion to grant equitable relief in the form of an interim or final injunction against a U.S.-based Cloud provider, to the extent that the Court cannot supervise compliance with its order under the rules of contempt of court.

Is data stored in the U.S. at any greater risk of being accessed by government than data stored in Australia?

Formal U.S. Government Requests

Private data stored in the U.S. is at a higher risk of being accessed by government agencies than data stored in Australia. In the U.S., formal requests by government entities in the form of subpoenas and warrants generally compel the provision of data and information. Under the Fourth Amendment to the U.S. Federal Constitution, which guards against unreasonable searches and seizures by the state, a warrant is issued only when the request is supported by probable cause that a criminal offense has been or is being committed, a description of the place to be searched and items to be seized is provided, and notice is given to the subject of the search.

However, Fourth Amendment protection is afforded only to information in which one has a reasonable expectation of privacy. The rationale is that once information is shared with a third party, that expectation of privacy ceases to exist. In the context of electronically stored information, the impact of this is extensive.

Subpoenas may be issued without showing cause by administrative agencies as well as private litigants. In recent cases, U.S. government agencies have relied on the 'Third Party Exception' to gain warrantless access to personal information, including:

1. the name, address, e-mail address and media access control address from Comcast Cable Communications of a person who used Comcast's Internet services in the course of sharing movie files online;⁴
2. the information on an individual's computer that was accessible by a peer-to-peer file sharing program;⁵
3. the chat account information from Yahoo! of a person who used Yahoo's internet services to access chat boards;⁶
4. the log-in information, including the date, time and IP address of each log-in, from Microsoft of a person who used Microsoft's MSN/Hotmail program;⁷ and
5. the contents of an iTunes files library shared over an unsecured wireless network.⁸

U.S. Government Surveillance

The power of U.S. government agencies to obtain information in any matter related to national security or terrorism has also expanded substantially in recent years through changes to the Foreign Intelligence Surveillance Act of 1978 ("*FISA*"). *FISA* sets forth procedures for, *inter alia*, requesting judicial authorisation for electronic surveillance of persons engaged in espionage or terrorism against the U.S. on behalf of a foreign power. The 2001 USA Patriot Act abolished the prior requirement that the "primary purpose" of the *FISA* surveillance be for the gathering of foreign intelligence and relaxed the standard so that the government now need only show that the collection of foreign intelligence is "a significant purpose" of the surveillance. The Patriot Act also amended the procedures for judicial oversight of *FISA* surveillance and expanded the definitions of "foreign intelligence information" and "agents of foreign powers." Under the current statute, there is no requirement that a target be engaged in criminal activity, although the government still must show probable cause that the "target of the surveillance is a foreign power or agent of a foreign power."

The availability of access without a warrant and the broad powers available under the Patriot Act have no parallel in Australian law. The scale of surveillance activity undertaken in the U.S., and the corresponding concern expressed by industry around the extent of expanding government powers, have not been mirrored in Australia. The U.S. also lacks a number of privacy protections and other limitations that constrain the ability of government agencies in Australia to compel access to data.

Broad new regulations being drafted by the Obama administration would also make it easier for U.S. law enforcement and national security officials to wiretap Internet and e-mail communications within the U.S. According to a recent article in the New York Times, the White House plans to submit a bill this year that would require all "communications service providers" to be technically equipped to comply with a wiretap order. The Times reported that government officials behind the proposal have not yet defined who would qualify as a "communications service provider," but officials have

suggested that the regulations may be applied broadly, including to companies that operate from servers located abroad.

Whilst some Australian government agencies possess powers similar to those held by U.S. agencies, the Australian government agencies' powers are only applicable in quite limited circumstances compared to the U.S.

Government Access to Data Pursuant to Mutual Assistance Treaty

Treaties between foreign governments also affect what kind of protection data enjoys, and become particularly relevant where data is stored in the Cloud. The U.S. and Australia have in place a *Mutual Assistance Treaty* that allows the countries' respective law enforcement agencies to gain access to data in the other jurisdiction in certain circumstances. The Council of Europe's *Convention on Cybercrime* is yet to be ratified by the Australian government, but has been ratified by the U.S. This means that Australian data stored in the U.S. is already subject to the European agreement and could be forcibly shared with the European signatories. If Australia also ratifies the European agreement, companies should be aware that Australian data hosted in a European Cloud will be exposed to access from other signatories, including the U.S. government.

What reputational risks will you assume by offshoring?

Within Australia, government, community and industry concern around data privacy is growing. The current federal government has expressed particular concern

about the potential exposure of personal data once it is transferred offshore.

The recent Exposure Draft which amends the National Privacy Principles flags a rising level of community and political concern around the issue, as well as the potential for new regulations over time. Any proposed offshoring would need to be supported by a clear PR and communications strategy in order to maintain credibility and able to refute actual or perceived security risks associated with the offshoring to a global Cloud.

¹ *Burger King Corp v. Rudzewicz*, 471 U.S. 462, 474 (1985) (quoting *International Shoe Co. v. Washington*, 326 U.S. 310, 316 (1945))

² *Rudzewicz*, 471 U.S. at 475.

³ *Rudzewicz*, 471 U.S. at 475.

⁴ *Worldwide Film Entm't LLC v. Does 1-749*, D.D.C., No. 10-38 (May 13, 2010); *Web User Lacked Privacy Interest in Account Data*, 9 PVL 768 (May 24, 2010).

⁵ *U.S. Perrine*, 518 F.3d 1196 (10th Cir. March 11 2008) No. 06-3336; <http://ca10.washburnlaw.edu/cases/2008/03/06-3336.pdf>; *Tenth Circuit Finds no Expectation of Privacy in Data Given Freely to ISP*, 7 PVL 418 (Mar. 24, 2008).

⁶ *U.S. v. Bynum*, No. 08-4207, 4th Cir. (May 5, 2010); *Yahoo! User Lacked Privacy Expectation in Account Data Shared with Yahoo!, Others*, 9 PVL 707 (May 17, 2010).

⁷ *U.S. v. Li*, S.D. Cal., No. 07 CR 2915 (Mar. 20, 2008); *No SCA Reasonable Privacy Expectation for ISP Customer IP Address, Log-In Data*, 7 PVL 501 (Apr. 7, 2008).

⁸ *U.S. v. Ahrndt*, D. Ore., No. 08-468, 2010 U.S. Dist. LEXIS 7821 (Jan. 28, 2010); *No Fourth Amendment, ECPA Privacy Claims in Documents Shared on Unsecured Network*, 9 PVL 257 (Feb. 15, 2010).

This paper was prepared by Freshfields Bruckhaus Deringer LLP as commissioned by Macquarie Telecom Pty Ltd. It is for general information only and is not intended to provide legal advice. Freshfields Bruckhaus Deringer LLP is a limited liability partnership registered in England and Wales with registered number OC334789. It is regulated by the Solicitors Regulation Authority. For regulatory information please refer to www.freshfields.com/support/legalnotice. Any reference to a partner means a member, or a consultant or employee with equivalent standing and qualifications, of Freshfields Bruckhaus Deringer LLP or any of its affiliated firms or entities.

About Freshfields Bruckhaus Deringer

Freshfields Bruckhaus Deringer is a global law firm with more than 470 partners and over 2,500 lawyers around the world. We have offices in China and other countries in Asia, Europe, the Middle East, and the United States and have worked with clients on their transactions in almost every country in the world. In jurisdictions where we do not currently have an office, we maintain excellent relationships with the leading law firms and work with them regularly.

About Macquarie Telecom

Founded in 1992, Macquarie Telecom is Australia's only business-specific hosting and telecommunications company. Working with and supporting some of Australia's best-known organisations including SBS, Cricket Australia, Webjet and the Australian Rugby Union, Macquarie Telecom provides data network services, mission critical hosting facilities and telecommunication services underpinned by industry-leading customer service.