FRESHFIELDS BRUCKHAUS DERINGER

macquarie TELECOM

RAJAH TANN

Lawyers who know Asia

The Cloud and Cross-Border Risks - Singapore

January 2011

What is the objective of the paper?

Macquarie Telecom has commissioned this paper by international law firm Freshfields Bruckhaus Deringer in collaboration with Rajah & Tann LLP to analyse the key risks associated with storing data in Singapore and 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 hosting service providers to offer Australian customers data storage in offshore jurisdictions through global or regional Clouds.

As some of the commercially available Cloud computing services are located in Singapore, this analysis compares Australian and Singapore 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 and a Cloud provider located in Singapore will typically provide standard contract terms that are governed by the laws of Singapore. For Australian customers considering a move to offshore data storage in Singapore, this has potentially wide ranging implications.

Can your data be sent offshore?

Regulated entities and financial services institutions in Australia should pay particular vigilance to any regulatory restrictions which may limit their ability to store their data offshore. For example, the Australian Prudential Regulatory Authority (APRA) requires authorized financial services institutions to notify APRA of any transfer of data offshore and to demonstrate that appropriate risk management procedures are in place to protect the data. The institutions must also secure guarantees in their contracts with the hosting service providers to allow APRA access and site visits to the services provider if required. Where the hosting service provider uses a number of offshore data centres to store the data, it may be reluctant to provide guarantees regarding data security and access of a sufficient standard to satisfy APRA.

In some circumstances, there may be a blanket prohibition on the transfer and storage of data overseas. For instance, the Commonwealth of Australia Government Contract for IT Services currently forbids suppliers from transferring or storing their customer data outside Australia (although a cloud computing strategic direction paper issued by the Department of Finance and Deregulation in January 2011 does contemplate a liberalisation of this prohibition and poses a risk based assessment).

How do you effectively maintain compliance across multiple jurisdictions?

Data hosted in an offshore Cloud may be stored in several locations across multiple foreign jurisdictions, which may limit your visibility over your data at any particular time. This may create difficulties in ensuring your continued compliance with Australian law and regulatory requirements.

A lack of consistency in data privacy laws across jurisdictions makes continued compliance with Australian law particularly difficult to monitor. The risk of non-compliance with Australian privacy laws is exacerbated by Singapore's lack of a unified and comprehensive regime for data protection and Singapore does not constitutionally recognise a general right to privacy. This is a key disadvantage to storing data in Singapore. Without a comprehensive data protection law, storage of your data in Singapore may cause your customers to have concerns about the standards of data security and available protection of their data. This may have serious reputational consequences and commercial implications for your business. It also carries risk implications in terms of your ongoing compliance with the Australian National Privacy Principles. The Australian Government's recently released Exposure Draft, if enacted, will introduce vicarious liability whereby if a business holding "personal information" in Australia discloses that information to an offshore entity such as a Cloud provider, it may be vicariously liable for any misuse of that personal information by the offshore entity, in this case the Singapore Cloud provider. Given the disparity in the privacy regime between Singapore and Australia, this may prove to be a tangible issue for Australian businesses and should be factored into any business case for offshoring data to Singapore.

Whilst it may be possible to impose compliance reporting or audit provisions in your agreement with the offshore Cloud provider (to track compliance with Australian laws), the costs of this are likely to be passed on to you and your Cloud provider may not be prepared to or able to guarantee compliance with Australian laws.

What Singapore laws might apply to my business?

160+ Disparate Statutes Regulate Data in Singapore

In addition to compliance with Australian law, businesses offshoring data to Singapore will have to comply with over 160 disparate, sector-specific statutes that regulate the use and disclosure of data management in Singapore including in relation to consumer protection laws, employment laws, e-commerce, telecommunications regulations and other industry specific laws particularly in health, banking and insurance. Any failure to store data offshore in the manner required by applicable Singapore laws may necessitate a restructuring of your data storing arrangements which may be expensive and disruptive. Furthermore, you may be exposed to the risk of non-compliance with Singapore laws which may have dire consequences to your business including wide reaching penalties such as fines, revocation of operating licences and other regulatory privileges, as well as adverse effects on your reputation.

Stringent data management laws in banking

Requirements for data management and protection are especially stringent in the banking industry due to the sensitive nature of customer information held by banks. Banks in Singapore owe a statutory duty of confidentiality to customers under the Banking Act which prohibits banks and its officers from disclosing confidential customer information, unless expressly permitted by the Act. The Monetary Authority of Singapore (MAS) has issued Circulars and Guidelines setting out the risk management and data security framework that banks are expected to implement in managing their data. Appropriate security solutions to address the risk of data theft, data loss and data leakage from endpoint devices, customer service locations and call centres, whether domestic, overseas or under outsourcing arrangements should be implemented. MAS expects banks to formulate a definitive plan containing specific implementation dates to achieve the security targets. MAS' Internet Banking Technology Risk Management Guidelines require deployment of strong cryptography and authentication mechanisms to protect customer data and transactions. If an Australian business is deemed to be a financial institution to which these laws apply, such a business will need to understand these specific laws and guidelines and comply with them. This could lead to complex legal issues for Australian banks storing data in Singapore if, for example, under Australian law there is a duty to disclose customer information but such a disclosure would be a breach of the Singapore Bank Act.

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

Hosting a transactional website on a server located in Singapore may expose you to Singapore income tax if the hosting arrangement amounts to a permanent establishment ("PE") where you are deemed to: (i) have a fixed place of business in Singapore; and (ii) carry on business activities (wholly or partly) through the fixed place of business. However, even a company without a PE in Singapore could still be liable for income tax if it has 'substantial business activities' in Singapore which create a source of income in Singapore. What constitutes 'substantial business activities' will be decided on a case by case basis but could include circumstances where, for example, a website hosted in Singapore results in substantial sales to Singapore customers. If considering whether to store data in Singapore, Australian businesses should obtain advice regarding their set up and operations to determine whether their business will involve a level of economic connection to Singapore that will give rise to a tax liability.

The precise tax liability of the PE will depend on the relevant Singapore and Australian domestic income tax laws as well as the extent of any relief provided under the terms of the Singapore-Australia Avoidance of Double Taxation Agreement ("DTA"). Certain types of expenditure, such as software payments, may qualify for deduction or capital allowances, depending upon the circumstances.

Where an Australian entity conducts business in Singapore that involves making taxable supplies, it is required to register for Goods and Services Tax (GST) if the turnover of its goods and services in Singapore exceeds or is expected to exceed S$1 million in any calendar year. Penalties will be imposed for failure to register. The supply of taxable services is chargeable to GST at 7%.

Service fees paid by an Australian business to a Cloud provider in Singapore may be subject to withholding tax. To the extent withholding is required, the Cloud provider could demand that it receive a net sum equal to the amount of its fees and that you gross up as necessary to cover any withholding tax.

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

There are inherent difficulties in effectively enforcing your rights against a hosting service provider in Singapore. You may not be able to avail yourself of the statutory rights and remedies arising under Australian law, as they would not necessarily have extra-territorial effect in Singapore. In Singapore, only foreign judgments which are for a fixed and ascertainable sum of money are enforceable under the Reciprocal Enforcement of Commonwealth Judgments Act ("RECJA"). The foreign judgment is not automatically recognized in Singapore, but needs to be registered with the courts in Singapore before it can be enforced. Prior to registration, the defendant may raise a number of defences against the recognition or enforcement of the foreign judgment. If any of the defences succeed, the foreign judgment will not be recognized or enforced in Singapore.

For all other Australian court judgments, (e.g. interim judgments, orders for specific performance and other judgments not for fixed sums of money) new proceedings have to be filed in the Singapore courts, citing the Australian judgment as the cause of action. These new proceedings will incur additional expenses and there is no guarantee that you will be able to obtain a valid, enforceable Singapore judgment.

Similarly, there are also inherent difficulties in seeking to enforce an Australian arbitral award in Singapore. There are certain circumstances where the defendant may successfully request that the enforcement of the Australian arbitral award be refused.

Is data stored in Singapore at any greater risk of being accessed by government authorities than data stored in Australia?

Police Powers under Computer Misuse Act

There is a tangible risk that data stored in Singapore may be exposed to extremely onerous police investigative power granted under the Computer Misuse Act. The Computer Misuse Act empowers any police officer who has reasonable cause to suspect that a computer is or has been used in connection with any offences under the Computer Misuse Act to: (i) have access to and inspect the operation of the computer at any time; and (ii) with the consent of the Public Prosecutor, require the person having charge of the computer to release information sufficient for the police officer to decrypt scrambled data held in the computer for inspection and investigation.

The territorial scope of the Computer Misuse Act is far-reaching and extends to any person regardless of his nationality or citizenship, even if the offender was not in Singapore at the material time of the commission of the offence, provided that the data itself was then in Singapore.

In light of the breadth of the police powers under the Computer Misuse Act, in the event that a Cloud provider is subject to any investigation, there is a possibility that your business data (and that of your customers) may be accessed for the purpose of such investigation.

General police and government investigative powers

In general, Singapore law grants extremely wide-reaching powers of investigation to compel the disclosure of data, including encrypted data, to government bodies and law enforcement agencies for the purpose of criminal enquiries.

Under Singapore's anti-terrorism legislation, there is a duty to disclose information to the police where there is reason to believe that national security, public safety, order or interest are at issue.

Disclosure of data for the purposes of public interest extends to the discovery process in civil court proceedings, where the court considers that the administration of justice would be frustrated by the withholding of information stored in Singapore which needs to be disclosed if justice is to be done.

The Singapore High Court recently held that a court order made against a bank requiring disclosure of customer information would prevail over the duty of confidentiality under the Banking Act (VisionHealthOne Corp Pte Ltd v HD Holdings Pte Ltd). Data stored in Singapore risks being subject to disclosure even where this may conflict with your obligations for data confidentiality under Australian privacy laws.

Therefore, you should consider that data transferred and stored in Singapore may be at a greater risk of being accessed by the government and law enforcement agencies, than data stored in Australia.

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

Australian businesses may fall under the jurisdiction of the Singapore courts where the Singapore courts find there is a sufficient nexus (established on the facts) between the dispute and Singapore. The Singapore courts may also assert jurisdiction where you have agreed to submit to their jurisdiction in any contract between you and your Cloud provider.

The Singapore courts may grant leave to a Singapore Cloud provider to serve the originating process on you in Australia, or elsewhere. Any judgment obtained against you in the Singapore Court can be enforced in any state or territory in Australia pursuant to the Foreign Judgments Act, provided that the judgment is final and for a money award. An arbitral award awarded in Singapore can also be enforced against you through the Australian courts under the International Arbitration Act.

What reputational risks will you assume by offshoring?

There are increasing concerns over data privacy in Australia and the security risks involved in offshore data storage. The Australian government's cloud computing strategic direction paper issued in January 2011 highlights a number of these potential risks and issues including the legal and regulatory issues canvassed in this paper. The government paper also noted the lack of legal precedent regarding liability in the Cloud.

Any proposal to transfer data overseas for storage would need to be supported by an effective PR and communications strategy in order to promote confidence and credibility amongst customers and refute any perceived security risks. The additional resources required to conduct such a PR campaign, as well as the costs to your business arising, from reputational damage in the event of an overseas data security breach, should be carefully factored into your assessment of offshore data storage.

This paper is prepared by Macquarie Telecom in conjunction with the international law firm, Freshfields Bruckhaus Deringer LLP and Rajah & Tann LLP, which has provided input on the non-Australian law issues. 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. Rajah & Tann LLP (Registration No. T08LL0005E) is registered in Singapore under the Limited Liability Partnerships Act (Chapter 163A) with limited liability.