



Data Sovereignty and the Cloud

A Board and Executive Officer's Guide

Technical, legal and risk governance issues
around data hosting and jurisdiction

David Vaile, Kevin Kalinich,
Patrick Fair, Adrian Lawrence

Version 1.0 July 2013

Cyberspace Law and Policy Centre

UNSW Faculty of Law



Supported by



N E X T D C

BAKER & MCKENZIE

Data Sovereignty and the Cloud

A Board and Executive Officer's Guide

Copyright © July 2013

The authors and the Cyberspace Law and Policy Centre, UNSW Faculty of Law

This Short version omits references and sources. Full versions of this document with references and notes can be found at the following sites:

- ❖ <http://www.nextdc.com.au/>
- ❖ <http://www.aon.com/>
- ❖ http://cyberlawcentre.org/data_sovereignty/

Authors:

- ❖ David Vaile is from the Cyberspace Law and Policy Centre at the UNSW Faculty of Law, Sydney, and teaches Advanced Legal Research in the Law School. d.vaile@unsw.edu.au
- ❖ Kevin Kalinich is Global Practice Leader, Cyber Insurance, at AON PLC. kevin.kalinich@aon.com
- ❖ Patrick Fair is a partner at Baker & McKenzie Sydney office, and former president of the Law Society of NSW and the Internet Industry Association.
- ❖ Adrian Lawrence is a partner at Baker & McKenzie Sydney office, and author of the LexisNexis loose-leaf service *The Law of Ecommerce*.

Acknowledgments:

Note that responsibility for the content of this paper is solely that of the authors, and not those named below. Co-authors may not necessarily endorse every statement included in every section.

Thanks to the following for generous contributions towards the creation of this document:

- ❖ NEXTDC <http://www.nextdc.com.au>
- ❖ Baker & McKenzie <http://www.bakernet.com>
- ❖ AON <http://www.aon.com>

Thanks to the following for helpful support and suggestions:


- ❖ Alison Cook, postgraduate researcher, UNSW Law Faculty
- ❖ Prof Graham Greenleaf
- ❖ Interns including Tim Chiang, Sasha Kolodkina, David Lee, Felix Lim, Lauren Loz, Peter Matuszak, Ryan Ruslim, Tia Singh, Cassandra Switaj (Bond U), Alice Yang, Bonnie Yiu (UTS).

Cover image:

- ❖ ID 6387708 licensed by Yay images, Norway from HappyStock, <http://www.yaymicro.com>

Trademarks

All trademarks and registered trade names are the property of their respective owners.

This is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Unported License. Contact us for licence for commercial use. <http://creativecommons.org/licenses/by-nc-nd/3.0/> 

[Some versions of this report are simplified by the omission of the extensive notes and references in the full version. Retrieve the online version above for our sources, and potential corrections and updates.]

Contents

Will you cope when your data has left the building (or the country)?	1
1. Cloud Computing and Data Sovereignty	3
2. Types of Cloud Services	7
3. Risk Management, Corporate Governance and Insurance Issues	11
4. Overview of Obligations.....	24
5. Third party access by legal means: Does it matter where your data is stored, or by whom?.....	27
6. Security Considerations	42
7. A Cloud Data Location and Jurisdiction Policy?	46
8. Pulling it All Together.....	51
9. It's not too hard!	53

Contents in detail

Will you cope when your data has left the building (or the country)?	1
1. Cloud Computing and Data Sovereignty	3
Introduction	3
Why are cloud sovereignty and data jurisdiction important?.....	4
What is cloud data?.....	5
What do generic cloud data location or jurisdiction policies cover?	6
2. Types of Cloud Services	7
Cloud Service Models.....	7
Cloud Delivery Models	8
Real world: A mix of models and risks.....	9
3. Risk Management, Corporate Governance and Insurance Issues	11
Cross-department Coordination	11
Data Sovereignty Risk Management Issues.....	12
The Australian Experience.....	13
The Potential Impact of Foreign Regulatory Requirements.....	14
Managing Data Sovereignty Risk through Prudent Corporate Governance.....	16
Initial Selection of a Cloud Vendor	16
Negotiating the Cloud Contract	17
Minimizing Data Sovereignty Risk Through Appropriate Insurance Coverage.....	20
Risk Mitigation – tips for CIOs	22
4. Overview of Obligations.....	24
Legal obligations: statutory, case law and code compliance in Australia	24
Steps to assess a data set for local or out of jurisdiction data storage or control	26
5. Third party access by legal means:	
Does it matter where your data is stored, or by whom?.....	27
Introduction	27
Background	28
Different Types of Data Requests.....	28
Limitations on Searches and Seizures under the 4th Amendment of the US <i>Constitution</i>	30
<i>USA Patriot Act</i> of 2001.....	31
<i>Foreign Intelligence Surveillance Act</i> of 1978 (FISA)	32
‘Administrative subpoenas’ such as National Security Letters (NSLs).....	34
<i>Electronic Communications Privacy Act</i> of 1986 (ECPA).....	35
Secret Surveillance Programs.....	37
Data Access Demands in Litigation	38
Access Requests on Behalf of Foreign Governments regarding International Assistance	39
Analysis	40

6.	Security Considerations	42
	Never-ending Stories of Data Breaches Focus the Mind on Security.....	42
	Two key IT security issues for the cloud.....	42
	Cloud Computing Security Considerations – Checklist (DSD).....	43
	Cloud security more generally	45
7.	A Cloud Data Location and Jurisdiction Policy?	46
	Developing internal cloud data location and jurisdiction policies	46
	Who else should be responsible for digital document location and jurisdiction policies?	47
	Creating a Policy	48
	How do you develop a policy to deal with all these issues?	48
	Guidelines: what should be included?	48
	Classification of data	49
	Data Accessibility	50
8.	Pulling it All Together.....	51
	Interaction with your tools and other policies.....	51
	Implement and integrate	51
	Audit and evaluation	51
9.	It's not too hard!	53

Will you cope when your data has left the building (or the country)?

“Cloud computing is a new way of delivering computing resources, not a new technology.” Recent legal and business developments mean renewed attention is being directed to issues arising from storage of business and personal data in the cloud in Australia, the US and around the world. Questions such as the following are becoming common:

- ❖ How can cloud services be used safely, and when can they be dangerous?
- ❖ What is ‘data sovereignty’ in the cloud? Does data know or care about legal jurisdiction in the cloud, or is cyberspace somehow beyond such administrivia?
- ❖ What happens if you ignore data sovereignty in the cloud? Does it really matter where data is stored, or by whom?
- ❖ Will you be able to rely on cloud data stores when you need them? Will you be able to protect them against unwelcome adverse access or retrieval by parties other than the data owner and their authorised agents?
- ❖ In a court case, could you prove and exercise your/the owner’s rights to control, access or delete data held in the cloud?

Do you have a policy?

Many organisations don’t have an adequate policy in this area. Their existing document or data management policies may not cover *jurisdiction or location*, nor recognise challenges thrown up by a somewhat chaotic, hybridising cloud services environment. Does your company have:

- ❖ Staff sure of the differences between various cloud models and implementations, which data to keep in your home jurisdiction for legal or other reasons, and which data can be safely left to the vagaries of the international cloud?
- ❖ A clear policy for digital document retention and destruction in the context of the cloud?
- ❖ Specialists tasked to implement and maintain such policies and protocols?
- ❖ Hardware or software systems which enable last-resort access to data stores created with obsolete, deprecated or compromised cloud tools?
- ❖ Awareness not only of ‘big data’ cloud location or control issues but also those associated with BYOD or ad hoc clouds?
- ❖ A litigation plan to provide ‘discovery’ over all your cloud-hosted data, and to protect certain elements of it from unwarranted or unproven claims for such access?

Are cloud and data location polices too hard?

Some suspect that data sovereignty and access issues can impact on their organisation's performance and reputation, but are tempted to use the 'Too Hard' basket. This is not a survival strategy. With a guide like this and some advice, anyone can follow a structured approach providing business benefits as well as protection from unforeseen hazards in the cloud.

Complex legal, technical and business risk issues raised by cloud data sovereignty can also be an excuse for shifting the blame between IT, legal and corporate departments. It is critical that you know who is talking to whom, and that everyone knows where the buck stops.

Our audience

This paper looks at issues affecting data sovereignty in the cloud, and suggests how to create protocols for managing the potential risks and rewards of handling the new cloud services safely.

Is this for legal departments, finance, risk managers, IT, corporate executives, someone else, or all of these audiences? Probably "all of them".

Anyone participating in corporate governance or operations which involve understanding cloud data storage and usage risks should find this paper of value.

Although there are limits on how far we explore technical issues, in some places we offer legal or technical detail which will not interest everyone. Don't let this put you off. You should be able to get the gist and move on.

The focus is primarily on the Australian jurisdiction, but the principles in government policies, standards, case law and even legislation are increasingly being reflected in different jurisdictions around the world. Companies operating in Australia may also be confronted with similar issues in other countries, and some countries play a more central role in the cloud industry than others.

Accordingly, we offer international equivalents or comparisons in certain sections or footnotes, though these are by necessity illustrative, rather than exhaustive. You can also see the References section at the end for a consolidated list of these comparative references.

[Some print versions of this report are simplified by omission of the notes and references in the full version. Please retrieve the online version to follow up our sources.
See inside cover for details.]

1. Cloud Computing and Data Sovereignty

Introduction

Legal and business developments, and the replacement of local servers by outsourced remote services as the main information-hosting model for modern business, mean that a spotlight is shining into the dark recesses of the corporate computer cupboard. Seemingly innocuous questions are emerging with ever more serious implications:

- ❖ How can cloud services be used safely, and when can they be dangerous?
- ❖ What is 'data sovereignty' in the cloud? Does data know or care about location or legal jurisdiction in the cloud, or is cyberspace somehow beyond such administrivia?
- ❖ What happens if you ignore data sovereignty? Does it really matter where data is stored, or by whom?
- ❖ Will you be able to rely on cloud data stores when you need them? Will you be able to protect them against unwelcome adverse access or retrieval by parties other than the data owner and their authorised agents, from within or outside Australia?
- ❖ In a court case, could you prove and exercise your/the owner's rights to control, access or delete data held in the cloud, wherever and by whoever held?

How do cloud legal issues in relation to jurisdiction or location differ from those arising from conventional outsourcing or hosting?

It is easy to exaggerate the difference a cloud makes. In many ways the issues start from the same foundation. Traditional hosting or server hire contracts involve use of someone else's storage or computers. "But it would normally have been clear who you were dealing with and where your rented resources were. Such arrangements were also unlikely to have been established on a casual or informal basis. With cloud computing, however, the location(s) of your data [and under whose jurisdiction they fall] may be unclear, possibly even unidentifiable and it is also much easier to set up such an arrangement. The ease with which cloud resources can be allocated and reallocated makes it more likely that it will be done without an appropriate review of the relevant legal issues."

Are cloud data location and jurisdiction polices just too hard?

Some governance-level managers and directors have an inkling that how they deal with cloud data could, if things go awry, have a big impact on their organisation's performance and their professional reputation. The potential benefits are widely touted and frequently quite achievable, while the risks, costs and uncertainty aspects are less well known. But managers and directors may be tempted to pass this aspect off to the 'Too Hard' basket, or hope that someone else is taking care of it.

This is often no longer a survival strategy. The risks can now be too great. With the help of a guide like this supplemented by expert advice on specific issues as necessary, virtually anyone can address most of the core issues in a structured approach that provides substantial business benefits as well as protection from the more obvious cloud jurisdiction hazards.

Do you have a policy?

Many organisations don't have an adequate policy or a practical system for dealing with the questions raised by cloud data. Their existing document management policy may not cover the technical realities of digital versions of documents, or it may not recognise the challenges thrown up by the hybrid document environment (part paper, part electronic, part chaos).

A negative answer to any of the following questions may mean that your company (or client) is not sufficiently managing its digital documents.

Does your company have:

- ❖ A clearly articulated policy for cloud data location or jurisdiction?
- ❖ Employees who know which documents they should keep locally or under local control for legal reasons, and which they can safely allow out of the jurisdiction from day to day?
- ❖ Specialist individuals specifically tasked with the responsibility of implementing and maintaining protocols for cloud data location or jurisdiction decisions?
- ❖ An internal committee that reviewed your policy within the last 12 months, or that tested your protocols within the last 12 months?
- ❖ Hardware or software that enables retrieval and access for remote cloud data sets processed with obsolete systems?
- ❖ A policy for cloud data location or jurisdiction that covers not only the core of office servers, desktops and laptops, but also BYOD, 'ad hoc' clouds, and personal peripherals like home computers, smart phones, and tablets of staff and key consultants?
- ❖ Its policy and protocols periodically assessed by objective third parties for review and validation?
- ❖ A plan in place in the event that litigation or law enforcement action is commenced, where your company can expect to be required to provide discovery over some or all of your data in various locations and jurisdictions, arising from action in Australia or in another jurisdiction?

Who talks to whom -- where does the buck stop?

The complex legal, technical and business issues converging on cloud can easily be used as an excuse for shifting the blame (for instance between IT, legal and corporate departments). These complexities mean it is critical you know who is talking to whom about it, and that everyone knows where the buck stops.

Why are cloud sovereignty and data jurisdiction important?

Most documents are now digital and networked

Once removed from the physical constraints of hard copy, networked digital documents can be copied and moved between locations or jurisdictions with trivial effort.

Foreign litigants and governments have a much easier time getting access to your data if it is within their jurisdiction

While there are international or inter-country arrangements which enable access in or from other countries, most countries favour access requests made in relation to local documents, or documents under the control of entities over whom they have jurisdiction.

Laws in other countries may be quite different from those in your own country.

Third party legal access options, including detailed comparisons of mechanisms for such access under Australian jurisdiction and under that of the main cloud hosting forum, the US, are complex, so we discuss some examples in Chapter 5.

Cloud data storage contracts may be on terms unfavourable to users, or silent on key issues

Particularly for Web-grade IaaS (see below for cloud acronyms), service provider business models may rely on excluding liability for matters which may be within their control.

Typical SaaS host models may also depend escaping liability for such matters.

Some countries or jurisdictions may have much worse IT and data security or privacy protections for your data than Australia's, or their protections may be harder for subjects or owners to use

The evolution of business, legal and technical support for adequate online security, confidentiality, privacy and/or data protection vary greatly from country to country. International agreements such as the *Convention on Cybercrime* from the Council of Europe (CETS 185, in force in Australia from March 2013) arose to address this in some areas. But many countries are not a party to relevant agreements; some of them also have quite underdeveloped legal coverage of online issues generally.

And those who are parties to a Convention may have varying implementations of its model laws. The US and Italy for instance have exposed their citizens to less of the effects of the Convention than Australia has, meaning that rights and obligations may not be symmetrical.

Practical IT security implementations, or the degree of protection of Australian-owned data from third party access, will vary according to these and other local factors.

Increased scrutiny and professional liability

Inability to either produce data in response to legal request, or to protect it from unwanted demands from third parties, may create a significant governance impact.

Such an outcome, in the worst case, may mean not only is the future of the company at risk, but also the personal reputations of those directors or executives who drive the company.

Strategic importance to the organization: methodical solutions needed

The judicial gaze has begun to focus upon the entire stores of information held by companies, and how companies deal with those stores. Governments increasingly require transparency around IT security failures. And every Internet user has been alerted to the risk of their data being subject to access by unwanted parties.

Corporations that do not have in place strategic, comprehensive and reasonable data storage, location and jurisdiction policies, methodically and consistently adhered to in implementation, choose to chance a fate serious in its potentially destructive outcomes, if the ire of judicial, regulator or market condemnation falls upon them.

What is cloud data?

The modern corporation generates a plethora of digital documents, all of which are now candidates for, or generated by, cloud storage. For example:

- ❖ Imaged versions of original paper documents
- ❖ Files (including word processing, spreadsheets, presentations)

- ❖ Email (including email messages, instant messages, logs and data stores)
- ❖ Databases (including records, indices, logs and files)
- ❖ Logs (including accesses to a network, application or Web server, customer tracking or profiling)
- ❖ Other forms of meta-data
- ❖ Web pages (whether static or dynamically constituted)
- ❖ Audio and video recordings and streams
- ❖ App data sets
- ❖ Software itself may constitute a significant cloud data holding
- ❖ Access control information and passwords
- ❖ And others too numerous to mention!

What do generic cloud data location or jurisdiction policies cover?

Clearly data location and jurisdiction policies already exist in the non-digital world, and typically cover issues such as those below, which remain relevant for online documents:

- ❖ **Retention:** keeping the records in one form or another.
- ❖ **Destruction:** destroying the originals and copies, in some cases with detailed logs of the name and content of destroyed documents.
- ❖ **Coverage:** not every scrap of data warrants formal treatment.
- ❖ **Purpose:** the reason or purpose for decisions to store at all, or to prefer storage inside or outside the jurisdiction.
- ❖ **Process:** the means and media for putting cloud data location or jurisdiction decisions into effect, with associated protocols and worksheets.
- ❖ **Timing:** the various periods' data must be held for in any relevant jurisdiction.
- ❖ **Responsibilities and plans:** clear documentation indicating who is responsible, and procedures and routines to be followed.

2. Types of Cloud Services

Different cloud service models implement varied technical and processing attributes, so it is not surprising that they raise a range of different legal and policy issues around data sovereignty.

This section briefly names those different models, and some of their technical features or practical implication issues. (This is a very brief introduction; an extensive technical literature outside the scope of this paper explores the features of each model.)

Cloud Service Models

Cloud computing services come in three main Service Models, which vary according to the extent of the stack managed by the vendor compared with that under the control of the customer, and thus the level of interaction between the cloud service and the data it is holding.

Infrastructure as a Service (IaaS)

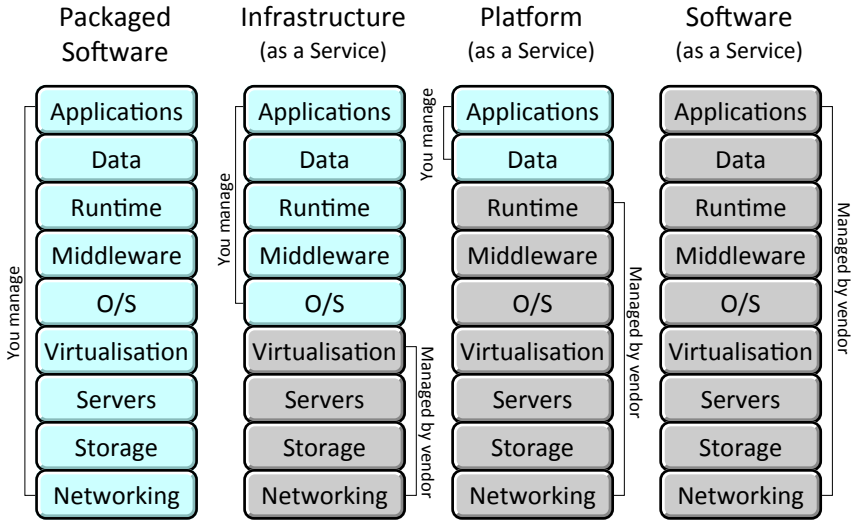
The relationship and interaction between the cloud service and the data may be small or minimal. With “Infrastructure as a Service”, the service is limited to the provision of the infrastructure needed. (Sometimes also called Hardware as a Service (HaaS).)

Platform as a Service (PaaS)

Interaction is medium when the cloud provider furnishes hosting and a platform, but not the specific applications. This model is known as “Platform as a Service.”

Software as a Service (SaaS)

The interaction may be large or frequent in “Software as a Service.” In this case, the customer has access to a wide menu of capabilities; the cloud provider furnishes hosting, storage, platform, as well as software applications for immediate use with the customer’s data. (Sometimes also called Application as a Service (AaaS).)



Cloud Service Models

Other Service Models?

Some commentators have suggested other Cloud Service Models. We offer them here for the purposes of completeness, though most of the literature, and this report, generally refer only to the three main types above (Infrastructure, Software and Platform).

Integration as a Service (IaaS)

This model transfers system integration functionality to the cloud, providing on demand data transport between internal systems and third parties (especially trading partners). Small and Medium Business (SMBs) use IaaS to enable B2B integration at low cost with a light IT footprint. IaaS providers include Amazon SQS, OpSource Connect, Boomi and Mule On-Demand.

Business Process as a Service (BPaaS)

Business Process as a Service (BPaaS), a.k.a. 'Business Process Management as a Service' (BPMaaS) refers to an emerging cloud service model whereby business processes (e.g., payroll processing or human resource) are delivered within a multi-tenant, self-service cloud service model through the internet via web interfaces and web-oriented cloud architecture.

Desktop as a Service (DaaS)

Also known as 'hosted desktop services' or 'virtual desktop', DaaS is a multi-tenant architecture based on outsourcing a virtual desktop infrastructure to a third party provider. The service provider manages back-end data storage, backup, security and upgrades, while a user's personal data is copied to and from their virtual desktop at connection.

Testing as a Service (TaaS)

This enables proof-of-concept or prototype testing prior converting an internal system to a cloud computing model, typically via a network emulator.

Management as a Service (MaaS)

Management as a Service enables management of cloud services such topology, resource utilization, virtualization and availability management. Common Cloud Management Platform (CCMP) contains business and operational management services for delivering cloud services in a self-service mode

Security as a Service (SecaaS)

This is delivery of secure platform and applications to clients on request. Users maintain their own personal security keys, but share responsibility with the provider.

Cloud Delivery Models

Cloud computing capabilities can be delivered and used in four different models: Public, Private, Hybrid, and Community (some commentators add variants to these). The choice of delivery model has significant effect on the nature, content, and terms of the cloud service contract.

Public Cloud

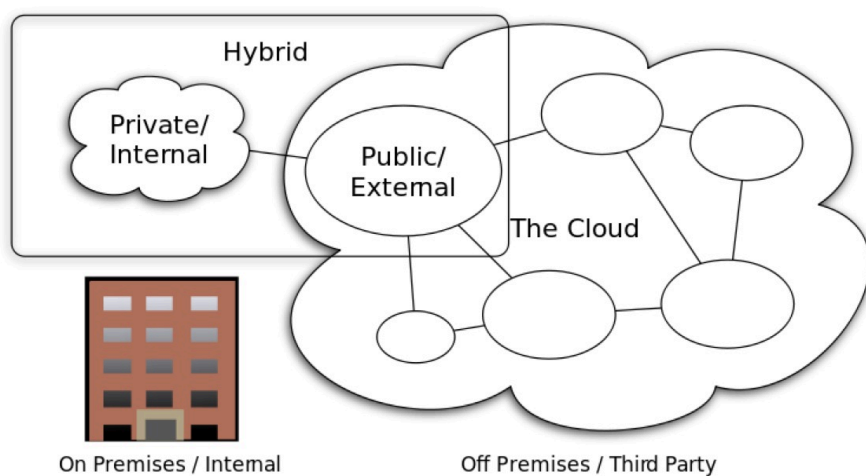
The public cloud infrastructure is made available to the public or a large industry group and is owned by an entity selling cloud services. It is potentially the lowest cost model, especially if at the 'Web-grade' rather than 'Enterprise Grade' end of the assurance spectrum. This is more accessible to small entities, but the terms and negotiability of the contract usually offer limited comfort.

Private Cloud

The private cloud infrastructure is operated solely for an entity. It may be managed by the entity or a third party, and may exist on premise or off premise. It is more attractive to larger entities and government because of their greater capacity to manage their part of the investment and support required.

Hybrid Cloud

The hybrid cloud infrastructure combines public and private clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability, such as when cloud bursting for load-balancing between clouds.



Cloud Computing Types

CC-BY-SA 3.0 by Sam Johnston

Community Cloud

This term is less commonly used, typically by government. The community cloud infrastructure is shared by several entities. It supports a specific community that has shared concerns, such as the same mission or policies, or similar security requirements or compliance considerations. It may be managed by the entities or a third party and may exist on premise or off premise.'

Some features and risk attributes are shared among all Cloud models, while others are more applicable to particular models. We only refer to a particular model if it is relevant for a particular risk or feature.

Real world: A mix of models and risks

The issues under consideration when we look at a particular Cloud implementation will vary depending on the service, the business, and the data held by the service. Most customers in reality use a combination of cloud service models depending on the type of service needed, the utility of the service offering, and the risk of the data.

- For example, in an Infrastructure as a Service (IaaS) arrangement, the service provider would not be expected to have any access to data at all.
- Some service providers also provide SaaS where all data is encrypted from the customer's desktop: this means data is not accessible by the service provider either.

This question of who can see the data, and on what basis, is important to the overall risk of putting data in the cloud, and should be a focus of your analysis. Service and Delivery Models are a useful framework for this work, but it is critical to understand the details of data access, and weigh up the actual risks of a particular Cloud implementation.

A related issue is important for discussions about access to data by regulators (including those discussed in Chapter 5 below): as a practical matter, law enforcement is unlikely to know that a particular company has data in one of the many cloud services operating in a jurisdiction, under whatever Model, so the best way to get data from a company can be to just directly order that the company deliver it up. Where the data is stored or hosted in a jurisdiction but the legal entity is absent from it, the risk that the cloud data will be located and accessed by law enforcement can be quite small.

It is also useful to give attention to the characteristics of the data, and the risk different data carries: only some classes of data are actually dangerous if lost. See discussions in Chapter 4 and Chapter 7 (under Classification) on this point.

There is of course typically the embarrassment of a data breach: note the recent finding by ACMA against AAPT, the new penalties, and the proposed new disclosure obligations in the *Privacy Act*. But it is also important to ask, how often is money or valuable data actually lost? The Verizon Data Breach Report has examples with detail of the types of breaches and the proportion where the information lost actually could cause loss. The incidence of loss, and the security response appropriate, will vary from case to case. (Chapter 6 discusses related issues.)

Having outlined the Models by which Cloud services can be categorised, and considered some of the real world complications which show that the devil is in the detail rather than the model, we turn now to a consideration of how this new world looks to the risk, governance and insurance specialists who have to assess what this all means.

3. Risk Management, Corporate Governance and Insurance Issues

This chapter explores the detail of issues which must feature prominently in the thinking of Risk, Governance and Insurance officers of any organisation considering cloud models and data storage questions. The May 2013 Privacy Alerts Bill (which would create a form of mandatory disclosure breach notification in Australia), the June 2013 disclosure regarding FBI/NSA top-secret PRISM data-mining of telecom and Internet providers, and the May 2013 Australian *National Cloud Computing Strategy* combine to elevate cloud computing to the top of risk management considerations.

Cross-department Coordination

Below we will examine the historical evolution whereby cloud service providers, like other external suppliers, rarely if ever act as insurers of a customer's business. Therefore, it is important that the exposures are adequately qualified and quantified, an approach at the heart of Prime Minister Julia Gillard's landmark national Security Strategy unveiled in January 2013:

“It will provide Australia with an expanded and more agile response capability to deal with all cyber issues – be they related to government or industry, crime or security, and create a hub for greater collaboration with the private sector, state and territory governments and international partners to combat the full strength of cyber threats.”

Data sovereignty analysis is not limited to the CIO. Legal counsel, finance/treasury, information technology security, corporate audit, procurement and risk managers, among others, need to implement responsible corporate governance and risk management practices, which are essential for companies using a cloud infrastructure. Businesses must balance the flexibility and potential cost savings of cloud computing with the risks inherent in storing data off-site, beyond the company's direct control, and possibly even in a foreign country with different laws.

Despite the benefits of flexibility, scalability, and cost savings that a cloud infrastructure offers, entities adopting this new methodology need to consider potential security and data sovereignty concerns. Cloud computing derives efficiencies from economies of scale through the sharing of costly resources by multiple entities, but it is this sharing of resources – particularly with the public cloud – that increases data security concerns. Another risk involves data sovereignty: The cloud provider may decide, for technical network efficiency reasons, to transfer data from one data centre to another, and these data centres may be located in different countries, or under the control of different jurisdictions.

Australia is the world's thirteenth largest economy, and the Australian e-commerce market continues to grow – predicted to increase to over \$37 billion in 2013. Nearly 9 million Australians shop online and, an estimated 97% of Australian Internet users have used the Internet to purchase goods. Entities in every industry sector – from Retail, Financial Institutions, Healthcare, Hospitality, Media, Communications, Technology, Consulting and Professional Services to Manufacturing and Education are considering cloud services to facilitate data usage.

However legal developments such as the Privacy Reform Act of 2012 increasingly regulate such adoption. Businesses which outsource to foreign service providers, such as cloud computing entities, must now take reasonable steps to confirm that the recipient complies with Australia's

privacy laws, and (unless an exemption applies) may be held strictly liable for non-compliance. The new law also requires an organisation's privacy policy to state whether personal information will be disclosed overseas and, if so, in which countries.

A company's CIO needs to engage her company's IT Security, privacy, risk management department and legal personnel to obtain detailed information from cloud providers concerning their security programs, including who can access the data, where it will be located (country of jurisdiction for evaluation of legal obligations), technical aspects of the infrastructure, and what steps the provider has taken to protect the integrity and security of the data.

Multiple client departments should coordinate to evaluate a range of information, including how the cloud provider erects security walls between data from different customers, who will have access to the information, whether encryption is possible, whether customers must be notified that their information will be stored in a cloud, whether the cloud provider has its own adequate insurance coverage (possibly name your company as an "Additional Insured"), and whether some information is simply too sensitive to turn over to a third party.

An added benefit of obtaining evidence of insurance from your outsourced provider is that obtaining such insurance would require the outsourced provider to be scrutinized by an insurance underwriting expert prior to obtaining its Cyber Insurance Policy.

(Our final Chapters below also offer suggestions for how to engage the different organisational 'tribes' in the necessary shared analysis and implementation of policies and processes which address emerging cloud jurisdiction-related issues.)

Data Sovereignty Risk Management Issues

There are many practical reasons a company or agency might be cautious about having its data transmitted beyond its own national borders, or held by entities under another jurisdiction's supervision.

Offshore data centres in distant locations are obviously more difficult to monitor than local ones. Moreover, some parts of the world are simply more vulnerable to natural disasters, wars, so-called "acts of God," or government intrusions. Chief among the multitude of concerns about cloud computing is the fear that a business could have its data transferred to or into the control of an undesirable jurisdiction, without its knowledge or approval, and become subject to unacceptable exposures and legal obligations.

The concept of "data sovereignty", introduced above, refers to both specific data sovereignty laws limiting cross-border data transfer, as well as the more general difficulty of complying with foreign legal requirements that may be more onerous, less clear, unknown to the user, or even in conflict with the user's own country's laws. If the server location or control is not disclosed by the cloud provider or if it is subject to change without notice, the information is more vulnerable to the risk of being compromised. Uncertainty on this point is a risk factor in itself.

In addition, some nations' data sovereignty laws require companies to keep certain types of data within the country of origin, or place significant restrictions on transmission outside the country of origin. Some jurisdictions' privacy laws limit the disclosure of personal information to third parties, which would mean that companies doing business in those countries might be prohibited from transferring data to a third-party cloud provider for processing or storage.

Information stored in a cloud environment can conceivably be subject to more than one nation's laws. Indeed, the legal protections applicable to a single piece of data might change from one moment to the next, as data is transferred across national borders, or to the control of a different entity. Depending on where the data is being hosted or by whom it is controlled, different legal obligations regarding privacy, data security, and breach notification may apply.

Where there is a lack of specificity, a business will often feel compelled to err on the side of caution and adhere to the most restrictive interpretation.

In some cases, this will mean that large categories of data may not be allowed to be transmitted beyond the country's geographic borders or outside its jurisdiction. As a result, some businesses are employing a hybrid cloud strategy which involves contracting with multiple cloud providers that maintain local data centres and comply with the separate, local legal requirements for each country.

The complexity of these various data sovereignty laws may make businesses reluctant to move to a cloud – especially a Public cloud, as described in Chapter 2 above, “Types of Cloud Services” – where it cannot restrict the geographic location or jurisdictional control of its data.

In concept, using a public cloud on a multinational scale should be highly flexible and cost-effective for a business. However, the multitude of data sovereignty restrictions to which a company must adhere creates a daunting challenge.

Despite the notable benefits, many companies can be reluctant to utilize cloud technology because of fears regarding their inability to maintain sovereignty over the data for which they bear significant legal responsibility. (See also Chapter 4, “Overview of Obligations,” and Chapter 5, “Third Party Access by Legal Means: Does it Matter Where Your Data is Stored?”)

The Australian Experience

The new Australian Privacy Principles created by November 2012 amendments to the *Privacy Act 1988 (Cth)*, appear to significantly change the test for personal data transferred out of Australia.

- The prior Principles required “reasonable efforts to ensure comparable security,” which is difficult to qualify or quantify.
- The new Principles require the outsourced third party service provider “comply with Australian law.”

The new standard is potentially tighter and testable. Thus, there may be an incentive to consider hosting in-country, or at least under a regime that is known to be even more rigorous than Australia's. In January 2013, Prime Minister Gillard announced that CERT Australia would soon be part of a new Australian Cyber Security Centre, which aims to develop a comprehensive understanding of cyber threats facing the nation and improve the effectiveness of protection; this may have the effect of raising the bar for expectations of effective security in Australia.

The use of cloud technology in Australia is in flux, as regulators hurry to keep up with the evolving technology and increasing popularity of cloud solutions. Moreover, Australia's information security law is comprised of a bewildering amalgam of federal, state and territory laws, administrative arrangements, judicial decisions, and industry codes, so evaluating the impact of cloud sovereignty issues in this context becomes difficult. (Changes are due in 2014.)

Nevertheless, cloud computing is definitely on the rise in Australia. A recent study revealed that more than half of Australian companies spend at least ten per cent of their IT budgets on cloud services, and 31% of companies spend over 20% of their budget on cloud solutions.

Australian banks and insurance companies are regulated by the Australian Prudential Regulation Authority (APRA), and are required to consult with APRA in connection with outsourcing computing services offshore. Other Australian businesses are required to comply with the Privacy Act and the National Privacy Principles, which prohibit the transfer of personal information to a third party outside Australia unless that country has equivalent laws or the

entity ensures appropriate protection for the data. Many state and territory privacy laws contain similar expectations.

Australian registered organizations are required to verify that they store personal data (Personal Information, or PI) only in countries with legal standards equivalent to Australia's. The regulating bodies of some Australian industries, such as banks and insurance companies, may, as a practical matter, require that data be hosted exclusively within Australia.

Government organizations in Australia, such as defence contractors, education providers, and healthcare organizations, are required to adhere to the requirements of the Australian Government Information Management Office (AGIMO). AGIMO has set forth issues to be considered by agencies who are exploring cloud services. These agencies generally prefer to use data centres within Australia in order to maintain physical jurisdiction over their most sensitive data.

Some cloud providers in Australia will commit to host services within national boundaries to alleviate these data sovereignty concerns. However, even if the data is hosted domestically, it is nonetheless conceivable that some service providing access to the data could be hosted in a foreign jurisdiction, or under the control of another jurisdiction.

The Potential Impact of Foreign Regulatory Requirements

Australian companies considering cloud services should consider legal developments abroad when assessing the relative risks and benefits. (See also Chapter 5, below.)

Cloud hosting on a global scale is often based in data centres in places like the US, central Europe or Singapore which offer cost and other benefits. It may often store data connected to EU as well and Australian citizens. Differences between the regulatory frameworks where data is hosted, where hosting companies are based, and where data subjects or data users are based can create complex compliance environments. Some aspects can present a legal risk that cannot be fully offset by contracts or technology alone.

EU

The European Network and Information Security Agency (ENISA) launched a report in February 2013 taking a 'Critical Information Infrastructure Protection' approach to cloud computing, which calls for better transparency regarding logical and physical dependencies, such as which critical operators or services depend on which cloud computing services.

The European Commission is also considering new data protection requirements that would effectively apply throughout the world, including in Australia, to companies active in the EU market or which host data about EU citizens. If these proposals were implemented, cloud providers with EU customers would be required to adhere to such legal obligations for all of their data holdings, including data hosted for Australian customers.

European laws impose some limits on cross-border data transfers. The existing European *Data Protection Directive* obligates entities to maintain the security of certain categories of personal data, and permits the transfer of such information outside of the EU only to those countries the EU considers to have satisfactory data protection laws or if the company to which the data is transmitted agrees to comply with EU law. As a result, data may not simply be transferred at all to a cloud provider with servers located in countries whose data protection laws do not satisfy EU standards.

US regulators, pointing to increasingly robust proposals for increased regulation domestically, have recently suggested that emerging approaches to data protection in the US are more consistent with the EU approach than is widely appreciated.

EU laws on 'discovery' for litigation purposes may be inconsistent with US laws such as the *USA Patriot Act* in some circumstances. This may lead to confusion or conflict over appropriate responses to requests for access for this purpose.

US

The United States has no nationwide data protection law, but it does regulate disclosure of certain categories of personal information to third parties through a variety of laws. The US government notoriously asserts extraterritorial claims on data that potentially affect non-US entities through the controversial *USA PATRIOT Act*.

Even companies which try to require their cloud providers to keep their data within the geographic borders of their own country cannot assume that they are subject only to their home country's laws because, in certain circumstances, cloud providers may be legally obliged to communicate information, including confidential personal information, to authorities.

For instance, if a company is based in a country which prohibits disclosure of personal information without the subject's consent, it could conceivably violate its own nation's laws if it complies with a demand by the US FBI to turn over information stored in a US company's cloud or in a cloud located within US boundaries.

There has been some progress in dealing with these troublesome issues. The US Department of Commerce and the European Commission jointly developed a "Safe Harbor" to streamline the process for companies to comply with the EU's Data Directive. Intended for EU and US companies which store data, the Safe Harbor is available for companies which adhere to the seven privacy principles outlined in the EU Directive. A similar Safe Harbor framework exists between the US and Switzerland.

Of particular concern to cloud computing customers are the requirements that data subjects be informed of data transfers to third parties, and be provided the opportunity to opt out. (The 2012 proposals for EU data protection, above, include increased emphasis on effective consent rights for data subjects, so this may continue to be relevant when and if these proposals come into effect in 2014 or later. There have also been criticisms of the effectiveness of Safe Harbor from a compliance perspective.)

Data may also only be transmitted to third parties who follow adequate data protection principles, thus obligating the cloud customer to ensure that its cloud provider operates responsibly.

(Chapter 5, below, compares in more detail the example of the operation of provisions enabling third party access to data held subject to US jurisdiction on the basis of location or control, with the position under Australian law, from the perspective of an Australian business hosting data in the cloud.)

Canada

Canada presents a complex situation, as its data protection legal landscape is a patchwork of federal, territory, and provincial laws. It has laws requiring that certain data stay not just within Canada, but also within specific territories and provinces. Of particular interest is Canada's assertion that its privacy laws apply beyond its borders. The Federal Court of Canada recently held that the PIPEDA law gives the Office of the Privacy Commissioner of Canada (OPC) the right to investigate complaints relating to the flow of personal information outside Canada, regardless of whether the company involved is Canadian. If personal information about Canadian citizens is involved, the country's privacy laws and the OPC's investigatory powers extend across borders to foreign-based companies.

No uniform standards

Many other countries have proposed or are in the process of developing new laws regulating data privacy and related matters, and there is little hope of a uniform, worldwide standard which companies could confidently follow to ensure compliance.

Breach notification laws, for instance, vary greatly from one jurisdiction to the next. Some companies resolve this concern by storing only public data on public clouds, and keeping confidential information within their own control. Nevertheless, even where the data remains within the geographic borders of Australia, it is possible that the provider is subject to the laws of another country.

In addition, data which is transferred outside Australia to one or more foreign countries may become subject to a variety of external laws. Business organizations which operate across borders face unique challenges in managing network security risk, and those which use cloud computing technology have even more complicated exposures. A recent Capgemini study revealed that management considers “issues with data sovereignty” to be the second most important factor – just after “fear of security breaches”, and before the raft of technical and management issues – in determining whether to adopt a cloud infrastructure.

Therefore, along with concerns about integration and business agility, businesses are starting to realize the serious and complex issues involving data sovereignty in the cloud computing context.

Managing Data Sovereignty Risk through Prudent Corporate Governance

A corporation may effectively control its most significant business objectives through thoughtful policymaking and vigilant administration. In the critical area of information technology – particularly those businesses eager to employ cutting-edge cloud computing technologies – management’s obligation to exercise sound business judgment is even greater. The most successful companies will thoroughly evaluate the relative risks inherent in the cloud environment and implement effective mechanisms to prevent and mitigate harm to their business. Remember, the new Australian privacy law imposes potential liability on Australian businesses for breaches of the Australian Privacy Principles by their offshore data storage contractors.



Governance and IT security risk

Initial Selection of a Cloud Vendor

The organization’s governance and risk management framework should reflect the areas of security concerns the cloud infrastructure presents. Commencing with the initial selection of a cloud provider, management should involve corporate security personnel, risk management professionals, and in-house legal counsel to conduct a thorough screening. Beyond merely

evaluating pricing and delivery expectations, the decision-makers should assess security and legal considerations. A recent Ponemon survey reveals that corporate security professionals are involved in the vetting process only 9% of the time, which is unacceptable.

The most common international standard for compliance and certifications is ISO 27001, which details requirements for “establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System.”

Since a business can outsource the work – but not necessarily the exposure or resulting liability – it should include all necessary stakeholders in the evaluation process and they should conduct a highly-detailed inquiry into the provider’s:

- ❖ financial condition
- ❖ infrastructure
- ❖ data centre locations
- ❖ security procedures
- ❖ hiring practices
- ❖ record of reliability
- ❖ experience with the customer’s systems
- ❖ breach notification protocols
- ❖ methods for preventing unauthorized access or introduction of malicious code
- ❖ disaster recovery plans
- ❖ insurance coverage, and
- ❖ similar practices.

Companies should meticulously document their efforts in selecting and monitoring their cloud provider, as this evidence could be useful in defending against legal actions for breaches and insurance coverage lawsuits.

Negotiating the Cloud Contract

The initial formation of the contractual relationship between a business and its cloud provider is the key point in establishing a relationship that will benefit, not harm, the business. For this reason, management should devote extensive attention to the negotiation of the cloud contract’s terms.

Standard form contracts?

As originally developed, cloud computing was intended to become a highly commoditized service that would provide high volume services at a relatively low cost. Consequently, many cloud providers offered only standard form contracts containing boilerplate terms heavily biased in favour of the cloud provider, which utterly failed to meet the cloud customer’s particular business needs. Indeed, some standard agreements contained provisions allowing the provider to change the terms at its sole discretion. The following is from the actual contract of a leading cloud computing provider:

“We are not responsible for any unauthorized access to, alteration of, or the deletion, destruction, damage, loss or failure to store any of, Your Content, your Applications, or other data which you submit or use in connection with your account or the Services.”

Negotiation?

As the technology has evolved, however, and as businesses are becoming more astute about the potential risks, more well-run companies are now insisting on negotiating the terms of the cloud contract in order to protect themselves from the most serious exposures. A company should focus on contract language which precisely sets forth the parties' obligations in a number of critical areas. Attention should be paid to empowering users to take responsibility and control where appropriate, not to become a passive participant.

Sensitive data, breach

In particular, the contract should detail all matters relating to the protection of sensitive data and fairly assign liability for inadvertent or negligent disclosures. Transferring protected information into a cloud means that it is no longer within the company's direct control, yet the company retains substantial legal obligations concerning the protection of that data.

Location

The cloud contract should specify whether and to what extent different types of data may be relocated outside the geographic borders for processing or storage, and the parties may wish to restrict the countries to which data may be transmitted.

At a minimum, the cloud customer should insist upon knowing the location of its data, particularly if information is transmitted to one or more foreign countries.

Employee Screening

Contract provisions requiring employee screening should be considered to minimize the risk of internal theft or sabotage. Expectations regarding passwords, user security protocols, and encryption procedures should be spelled out in the contract. The provider's strategies for preventing unauthorized third party access, as well as procedures for replacement, sanitization and destruction of damaged physical media should be considered and made a part of the agreement.

Breach Notification obligations

The cloud provider's notification obligations in the event of security breaches or attempted unauthorized intrusions should be specified. The provider's approach to handling of foreign government requests for information should be included as well.

Keep other customers out

The contract should also reference measures in place to prevent other customers of a shared cloud from accessing private data, including separation of servers or other technical means, or establishing claims to ownership of data.

Access by other entities

Finally, the contract should identify all other entities which will have access to the data, including suppliers and subcontractors, and require follow up notice when additional third parties are to be given access. Your primary cloud provider may host services onshore. However, some data or services providing access to the data may be hosted by a down level provider that hosts offshore. If there is a breach of contract, do you have jurisdiction to enforce the contractual obligations? This could be difficult to audit in an offshore data centre. Regardless of the degree of protection promised by the cloud provider, the security and confidentiality of information is ultimately determined by the weakest link in the chain.

Outages and Force Majeure

Particular attention should be devoted to the contractual terms relating to outages and their consequences. Service interruptions are foreseeable, and the contract should set forth expectations regarding notification to the customer and prompt investigation and restoration of service. In many businesses, loss of access to the cloud and the data it hosts can be catastrophic, so the cloud contract's *force majeure* clause is of particular importance. The *force majeure* clause is a common contract term that frees parties from their contractual obligations and liability when an event occurs that is beyond the parties' control, such as natural disasters, wars, or other significant uncontrollable situations that prevent a party from fulfilling contractual obligations.

The precise definition of a *force majeure* is typically set forth in the contract and may vary widely from one agreement to the next. For this reason, negotiating the precise definition of *force majeure* in a company's contract with a cloud provider could substantially shift the risk and cost of service outages. An expansive *force majeure* definition that excuses the cloud provider from performance and liability in the context of power failures, labour disputes, subcontractor issues – situations in which the cloud provider arguably has some control – will expose the customer company to greater risk. In contrast, a very narrow definition of *force majeure* lessens exposure for the customer and shifts responsibility to the cloud provider.

Disaster recovery

The provider's disaster recovery and business continuity plans should also be thoroughly evaluated and referenced in the contract. Perhaps the contract would require that back-up power generators be maintained or that a geographically distinct recover site be established. The contract can dictate mundane matters such as coordination between the provider and customer regarding the timing of scheduled outages for system maintenance. It can also be used to shift significant operational responsibility and financial liability from one party to the other.

Monitoring

A good cloud contract will also contain provisions allowing for effective monitoring of the cloud provider. However, contractual protections alone are insufficient to protect the cloud customer unless there is an ongoing effort to ensure that the security requirements are actually being satisfied. The cloud customer must possess a significant level of sustained control and visibility from the cloud provider regarding how the data is stored. A company's reputation could be ruined overnight if its cloud provider failed to ensure customer privacy or if frequent system failures interrupted business. Therefore, the agreement should expressly provide audit rights to allow the cloud customer, or its designated representatives, access to the cloud provider's premises. Remote monitoring capabilities could also be considered.

Termination

It is expensive and difficult to switch cloud providers due to differences in architecture, metadata models and other factor. It is also essential that the contract address the eventual termination of the relationship. How the cloud relationship will end, particularly the safe return of information should be spelled out in the contract. The cloud customer should insist upon arrangements that allow adequate time to find alternative services to avoid business disruption.

The 2012 abrupt closing by Doyenz of its rCloud service illustrated the need for contractual protections in the event a cloud provider suddenly ceases providing service. The affected rCloud customers were given less than thirty days to either retrieve their data or have it relocated to servers housed in the US.

Terms that require the cloud provider to fully return, destroy or otherwise sanitize certain categories of sensitive information at the termination of the relationship, including possibly the destruction of hardware to ensure full security may be warranted in certain contexts. The parties should also negotiate and agree upon a dispute resolution procedure and specify which jurisdiction would apply.

Loss shifting

The cloud contract may also provide the opportunity to shift liability to the cloud provider losses resulting from data breaches, including indirect losses. Businesses may seek to have their cloud provider indemnify them in the event that data loss or misuse results from the provider's or its subcontractors' acts or omissions, whether negligent or wilful. While cloud providers seeking to deliver low-cost services will normally be reluctant to offer indemnification, some large companies have been able to obtain through aggressive negotiation some very substantial indemnification commitments.

Insurance

The cloud contract may also be used to require the cloud provider to maintain, and provide proof of, adequate insurance for potential cyber-related risks. Cloud customers might require cloud providers to carry commercial general liability policies, professional liability (errors and omissions) policies, business interruption insurance, and data breach coverage. The customer should always address insurance issues in cloud computing situations, both as to the customer's own insurance policies and the provider's insurance.

As a matter of judicious corporate governance, management must maintain a sensible level of indirect control, through adequate contractual arrangements and steadfast oversight. Since the privacy and data security obligations remain the legal burden of the cloud customer, the terms of the contract and its subsequent monitoring are critical. Furthermore, the landscape is evolving. Most States in the U.S. have compulsory data breach notification laws, which have been the driver for demand of Cyber Insurance. As and when mandatory data breach disclosure laws are implemented in Australia and Europe, we will see demand for Cyber Insurance accelerate. Australia is a good opportunity because of its robust economy.

(In 2012, the Australian privacy commissioner and consumer group Australian Communications Consumer Action Network made submissions to the federal Attorney General in support of mandatory data breach notifications. A bill was tabled in May 2013, but it is unclear at time of writing whether an effective mandatory data breach notification regime will be established.)

Minimizing Data Sovereignty Risk Through Appropriate Insurance Coverage

Based on the foregoing, cloud service providers, like other external service providers, will generally not act as insurers of a customer's business, so it is important to accurately qualify and quantify the risks.

Without question, more sophisticated risk management efforts are required in light of Australia's changing environment and the increase of cloud computing. Notwithstanding a corporation's best efforts to select a competent provider, to negotiate a favourable contract, and to exercise vigilant oversight, there will always remain some level of legal exposure that can only be mitigated with insurance solutions.

The good news is that insurance carrier underwriters recognize that, in the vast majority of cases, the technology and security of cloud computing providers, which specialize and focus solely on technology and security, is far superior to that of the average company, whose primary focus is selling its products or services. Therefore, most insurance carriers may offer broader coverage at a lower price for entities that utilize cloud providers.

Coverage Under Existing Traditional Insurance Policies?

	Property	General Liability	Crime / Bond	K&R	E&O	Cyber
1st Party Privacy / Network Risks						
Physical damage to Data only						
Virus / Hacker damage to Data only						
Denial of service attack						
B.I. Loss from security event						
Extortion or threat						
Employee sabotage of Data only						
3rd Party Privacy / Network Risks						
Theft / Disclosure of private info.						
Confidential corporate info. breach						
Technology E&O						
Media Liability (electronic content)						
Privacy breach expense / notification						
Damage to 3rd party's Data only						
Regulatory privacy defense / fines						
Virus / Malicious code transmission						
Coverage Provided?		<i>* For reference and discussion only; policy language and facts of claim will require further analysis</i>				
Coverage Possible?						
No Coverage?						

If an organization is truly interested in protecting their systems and wants to receive financial compensation for downtime or other events that impact the financial statements, then they will investigate cyber insurance, which can protect cloud based assets. Amazon Web Services, for instance, recently allowed insurance underwriters into its facilities to inspect its data centres for such insurance claims.

Shrewd management will utilize a thoughtfully-crafted package of insurance products to protect its financial future and reputation. The definition of “Loss” in the insurance policy must include actions by regulatory authorities for violations of data sovereignty regulations:

“Loss also includes civil fines or penalties imposed by a governmental agency and arising from a Regulatory Action, but only to the extent insurable under the law pursuant to which this policy shall be construed. “

Some portions of a company’s cyber risks could possibly be covered under other more traditional insurance policies, such as Professional Liability, Commercial General Liability, or even traditional Property insurance policies. However, it is wise to consider specialized cyber risk insurance coverage in order to adequately cover all network security risks. Traditional insurance policies were developed long ago and do not typically contemplate exposures such as those discussed in this article. While some categories of losses might be covered under some policies, material gaps usually exist. In the US, insurers are filing declaratory judgment actions against their insureds to deny coverage for cyber exposures.

It would be unwise to rely upon a company’s existing insurance policies – negotiated well before the expansion of cloud technology – to cover the risks inherent in the use of third-party data services such as cloud computing. Insurers are becoming familiar with cloud-related risks, and for this reason, cyber-insurance policies may begin to draw a distinction. Policies, as currently written, might exclude cloud-related losses in the event of a security breach, depending upon

how terms such as “computer,” “system” or “network” are defined. Many Cyber Insurance policy base forms exclude coverage for losses due to third party cloud computing providers.

Therefore, it is imperative to expand the definition of “Your Computer System” to include your third party cloud computing provider:

“Your computer system means a computer system:

- (1) under the ownership, operation or control of an organization; or
- (2) which is owned, leased or managed by a third party, for the purpose of providing hosted software, platform, infrastructure or other cloud computing services, but only to the extent that such computer system provides support and services to the organization in connection with its business activities.”

Even specific cyber-insurance policies could be limited to coverage for network-related losses occurring within certain defined geographic boundaries, so companies utilizing cross-border cloud providers need to closely review policy language to ensure that losses that occur in other geographic locations will still be covered. Note that between 36% -- 62% of companies surveyed said that their data breaches involved mistakes by third parties such as outsourcers, cloud providers and business partners.

Insurers scrutinize the security protocols of insured companies before issuing policies, so it is not surprising that this scrutiny now extends to the third-party cloud providers used by many potential insureds. Pricing and policy coverage limits will undoubtedly depend upon the extent to which the cloud providers demonstrate adequate attention to reliability and security. The increased risk of aggregating enormous amounts of data with a third party, outside the insured’s direct control, must be evaluated against the potential benefit of a cloud provider focused on state-of-the-art security protocols. Quantifying these risks and benefits will likely prove challenging for insurers and their customers, requiring analysis and advice by professionals familiar with these highly-specialized insurance products.

Risk Mitigation – tips for CIOs

While cloud services can result in users losing control over how and where data is stored, CIOs can fortunately play a proactive role in partnering with risk management and legal to set up risk mitigation and transfer policies designed to address and limit not only the incidence, but also the most severe adverse consequences, of cloud computing data sovereignty risks. Some of the common ways this can be done include:

- ❖ **IT Use Policy Review** Audit and regularly review your reliance on different forms of technology (i.e. Cloud Computing, smartphones, iPads, USBs) and ensure that various uses of such technology (i.e. work, social media, personal use) are appropriately regulated in company IT and/or Social Media policies and guidelines.
- ❖ **Supplier Audit** Identify any organisational dependence on outsourced service providers (especially cloud service providers) and work with the IT Security and Risk Management Department to perform regular and systematic audits of third party security infrastructure and practices designed to protect against data sovereignty risks, unauthorized access, use and disclosure of confidential information. Ensure that you have transparency of downstream level providers
- ❖ **Training** Educate your mates regarding the evolving legal exposures for both companies and individuals where it has been found that there has been a serious or repeated breach of privacy under the recently enacted *Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth)* (Privacy Reform Act).
- ❖ **Contracts** Mitigate cyber exposures by developing consistent contractual allocation

of liability templates in both customer and supplier contracts which place obligations on contractual parties to satisfy the minimum data collection, use, disclosure, and security requirements under the Privacy Reform Act.

- ❖ **Data Breach Management** Although not mandatory under the *Privacy Reform Act*, consider the benefits of implementing a Data Breach Management Policy to address and outline internal corporate prevention, detection and incident response processes in response to a security breach. It could help in defending an allegation that the company failed to take reasonable care in handling a data security breach.
- ❖ **Cyber Liability Insurance** Analyse your property and general liability insurance policies and determine any potential gaps in existing coverage. You may want to consider specific Cyber Liability Insurance to fill any obvious gaps.

While there is an argument that portions of a business' cyber risks could be covered under other more traditional insurance policies, such as Property (e.g. business interruption from a computer hack) or Commercial General Liability (e.g. third party data privacy breach litigation), it is wise to consider specialized cyber risk insurance coverage in order to comprehensively cover all network security risks.

The Australian cyber insurance market consists of several carriers offering a variety of products that offer coverage for specific types of losses, including losses to intangible property (e.g., data), cyber extortion, costs of data restoration, employee sabotage, forensic investigation costs, breach notification expenses, credit monitoring, business interruption losses and third party litigation. The underwriters balance the preventive measures employed by insureds (e.g. IT security, contractual allocation of liability, employee training and corporate guidelines) with incident response protocols (e.g. qualified attorney, forensics, and remediation). Insurance limits are available in the range of \$100K -- \$1 million for small entities and \$1 -- \$100 million+ for large entities. The question is not whether there will be a breach, the question is: "What frequency and severity?"

[This chapter is based on the work of Kevin Kalinich from Aon. This report is for general informational purposes only and is not intended to provide individualized business or legal advice. The information contained herein was compiled from sources that Aon considers reliable; however, Aon does not warrant the accuracy or completeness of any information herein. Should you have any questions regarding how the subject matter of this paper may impact you, please contact your legal, financial, IT security or other appropriate advisor.]

[Some print versions of this report are simplified by omission of the notes and references in the full version. Please retrieve the online version to follow up our sources. See inside cover for details.]

4. Overview of Obligations

This chapter provides an overview of the sorts of obligations to host data in one jurisdiction or another that arise in typical situations. The next chapter gives more detail on specific examples.

This paper uses developments in Australian law as a starting point for examining these obligations, but the issues raised often have more general application. We also make reference to parallel or relevant US and European law. Similar challenges are emerging in these jurisdictions and in others around the world.

It remains to be seen whether the competing trends for international harmonisation or for local diversification of legal rules will win out, and whether data sovereignty will become a central and complex aspect of such obligations.

This section provides a short overview of legal and compliance obligations. The reader is invited to pursue

Legal obligations: statutory, case law and code compliance in Australia

There are a number of reasons you may *wish* to store data in certain jurisdictions, or with entities regulated or controlled under certain jurisdictions:

- ❖ Practical technical reasons relating to current uses (increasingly less likely as cloud services mature)
- ❖ Contractual obligations (especially with entities including governments which may be subject to stricter statutory obligations)
- ❖ Temporary, time limited obligations to retain locally for certain purposes
- ❖ Business reasons, including customer or partner expectations
- ❖ Security or confidentiality concerns not easily mitigated by contract, or where the hosting partner is unwilling to accept any responsibility for breach and risk assessment suggests such a risk is unacceptable

A well-crafted cloud data location or control policy must include a method of identifying and tracking such documents (either as whole categories, or on an individual document basis), and setting out practical criteria for their appropriate storage.

However, such a policy will also need to analyse the second major reason for the local hosting of data – where you are *required by law* to retain the data in the local jurisdiction, or under the control of an entity regulated by that jurisdiction. Such requirements will tend to fall into one of the following categories:

1. where a statute either:
 - ❖ specifically requires the retention of the document in the home country, or by entities under its control; or
 - ❖ operates in such a way that the document should be so retained or controlled in order to prove compliance;
2. where there are cloud data location or control obligations related to compliance with industry codes, or to satisfy industry regulators; or

3. where local hosting of, control of, or access to the document is required because there is a reasonable anticipation of litigation to which the document in question is likely to be relevant.

An analysis of the obligations on a specific organisation is beyond the scope of this paper, requiring detailed consideration of many facets of the operation of the entity, and its characterisation by various laws. A data location and control policy should include a survey of the specific requirements affecting each aspect of the business or agency.

Note that in Australia there are relatively few specific statutory requirements that data be stored on Australian territory. These include:

- ❖ Certain documents must be accessible at the registered office of a company.
- ❖ A workplace safety rule in NSW says a workplace safety policy must be held locally.
- ❖ A provision in the new *Personally Controlled Health Records Act 2012* (Cth) requires the health records be stored locally by a locally registered entity.
- ❖ There are conditions on trans-border data flow of personal information in the new *Privacy Act 1988* (Cth).
- ❖ (Obligations to ensure security, say under the *Privacy Act*, may not specify a country or jurisdiction, but there may be some practical effect if appropriate security cannot be delivered under a certain arrangement.)

Many sorts of data are not however subject to such clear location-based statutory requirements, and can be stored offshore, if this is consistent with other obligations and judgements.

Promises, promises

However, it is important to also consider the disclosures required in Australia at the point of collection, whether from expectations under the *Privacy Act* or other laws, or promises made for business purpose. An organisation's representations to its customers and public as to its data storage processes and practices can in effect create obligations. These may form a contractual basis for obligations that are not directly specified in statute, but which later come under the *Australian Consumer Law* s18 (the old s52 *Trade Practices Act*) and so cannot be 'misleading or deceptive'.

This issue of what promises are made to clients when the data was collected is quite an important one: it may be more important overall than laws requiring data to be stored in the jurisdiction.

An organisation needs to have a clear view as to whether it is acting within the scope of the position it has put to the public (or, of course, to which it is bound in its contracts) when it decides to store data in the cloud. Assurances or promises made to end users or customers must be taken into account in assessing the overall pattern of obligations regarding data storage and control.

(See also the next chapter for discussion of the context of such obligations in relation to the prospect of third party access.)

Steps to assess a data set for local or out of jurisdiction data storage or control

The core decision-making process for determining if a particular set of documents or data should be held or controlled 'locally' (whether in-house, or in cloud services under the home jurisdiction) or can be safely hosted in the cloud in or under the control of other countries involves going through the below step-by-step process in order to satisfy yourself that retention is *not* required.

Step	Response	Action
1. Is local storage and/or control required for current use?	❖ Yes ❖ No	Local Go to 2.
2. Is local storage and/or control required by contract?	❖ Yes ❖ No	Local Go to 3.
3. Is local storage and/or control required by law or regulation?	❖ Yes ❖ No	Go to 4. Go to 5.
4. Are there certain periods not yet expired, including statutory limitation periods, during which local storage and/or control is required on an interim basis, even if eventually free to be relocated?	❖ Yes ❖ No	Local Go to 5.
5. Is local storage and/or control required for business reasons?	❖ Yes ❖ No	Local Go to 6.
6. Is local storage and/or control required for litigation or other special circumstances?	❖ Yes ❖ No	Local Foreign Cloud

An actual decision-making process will of course often be more complex, and these issues will fit within broader strategy and design processes.

See also Ch 6 for examples of security-related criteria that may assist with some of these decisions.

5. Third party access by legal means: Does it matter where your data is stored, or by whom?

Where the chapter on Risk, Governance and Insurance offers an overview of high level issues for cloud data location, this chapter drills into a core question: the complex of factors and legal issues which influence whether third parties can assert their right to access your data hosted in either a local cloud (in Australian jurisdiction) or in an offshore cloud (typically through services based in the US, the main cloud hosting jurisdiction).

Its observations may help guide your assessment of whether these jurisdictional issues warrant consideration of a 'data sovereignty'-aware cloud policy.

Introduction

For some time, improved global networks and the Internet have enabled hosting service providers to store data in low-cost jurisdictions, or where close proximity to large markets and scale facilities can create economies of scale.

In deciding whether to host data overseas, prudent customers have typically considered the cost of the service, security, and the sovereign risk of the location.

After an initial rush of cyber-libertarian optimism that the Internet represents a return to the wishful thinking of the early 1990s in which 'cyberspace' was somehow beyond the bounds of earthly law, there is a sobering recognition that information is subject to the laws of the jurisdictions where it is held, or which regulate the entities who control or host it.

Data hosting customers are increasingly asking whether remote hosting will involve transferring data to a foreign legal environment that may bring new risks or create special concerns and customers may ask in particular:

- ❖ does the service provider ensure that the foreign host provides a service that complies with Australian standards for privacy and security?
- ❖ what are the implications of exposing data held offshore, or under the control of offshore entities, to examination by foreign law enforcement regimes or litigants?

Government data users in particular feel the pressure of these questions.

Such concerns may be exacerbated by the ability and practice of certain law enforcement agencies to inhibit or prevent owners of the data from knowing that their data has been accessed and is subject to examination.

Focus on these issues has intensified with the advent of "cloud" computing. Information held "in the cloud" may be stored in multiple locations, and in multiple jurisdictions. Cloud computing with global networks obscures the customer's knowledge and control of the regulatory risk associated with the jurisdiction/s where the data is held, or by whom it is held.

Where the customer is itself storing and managing the information of third parties, this lack of information represents a failure to achieve transparency. For many customers a failure to fully understand the issues and risks associated with potential foreign access to data held in a global cloud may be illegal.

Many of the commercially available cloud computing services are offered by US-based companies at present, so in this paper we consider the potential scenarios under which a US-based data hosting service provider may be compelled to provide access to stored data to third parties, such as US government authorities and private litigants. We also comment on comparable laws in Australia, and issues raised in relation to European countries.

(While this paper does touch on both US and Australian law and practice, it is not intended as an abstract academic comparison of the substantive laws of two arbitrary countries; this would be a somewhat misleading basis for an Australian company considering relevant business and regulatory risks in the choice between hosting data under Australian jurisdiction or under other those of typical commercial cloud services. We offer a few comparisons with certain Australian provisions as a context for this risk analysis. Even if local and cloud storage jurisdiction laws were identical, other practical factors are more burdensome dealing with third party claims to access an offshore data store. For instance the costs of legal action, enforceability of remedies, and investigation or monitoring of developments are all more problematic in another jurisdiction since a local entity will often not have any presence there.)

Background

As a practical threshold item, we note that the US government is usually interested only in matters that concern US interests, for example, payment of US taxes, crimes in violation of US laws and threats to US national security. Much of the information held in cloud stores under US jurisdiction on behalf of foreign data owners may be of little interest to them for this reason. But from the examples we consider in this summary, it is apparent that US authorities will not apply particular self-restraint in scenarios involving foreign jurisdictions and US interests.

Compliance obligations under foreign laws on US companies (or their foreign data sources) not to provide data to the US government are not recognized as a defence to information requests by US courts or authorities. Additionally, as many data owners would be aware, US authorities can in most cases also obtain data under international cooperation treaties through foreign governments (as can Australian authorities).

Different Types of Data Requests

Informal requests

US government agencies typically have investigative duties and authority under the statutes or regulations of their establishment. As a result, government agencies can approach individuals and companies (including data hosting service providers) with informal information requests. Many US companies are willing to comply with such requests, to cooperate with the US government on issues of shared interests (*e.g.*, fraud prevention on e-commerce websites) or to avoid contributory liability for illegal activities (*e.g.*, copyright infringement).

Some companies are also obligated to comply with certain information requests. For instance, financial service providers have to cooperate with certain regulatory agencies and provide certain records as a matter of statute, and telecommunication service providers have to provide access for law enforcement purposes under *CALEA*.

But, in the absence of such specific regulatory compliance obligations, individuals and companies do not have to answer to informal information requests from US government authorities.

Summons and subpoenas etc.

Most US government authorities are entitled under specific statutes to issue formal information requests – summons, subpoenas or other forms – which either have to meet certain minimum

conditions (e.g., IRS summons) or which are generally permissible so long as there is some relevance of the inquiry to the mandate of the requesting authority and the subpoena does not violate constitutional or statutory limits. For example, grand jury subpoenas issued by US attorneys are generally legal and compelling unless they violate the US *Constitution* or certain limiting statutes. Grand jury subpoenas also contain secrecy restrictions to protect the grand jury process from inappropriate influences.

The applicable limitations in the US *Constitution* and the *Electronic Communications Privacy Act (ECPA)* are discussed below in more detail, but for purposes of this summary it is important to note that information requests in the form of subpoenas are generally compelling, unless an exception applies. If an exception applies, the recipient of the subpoena can assert it and demand that the government narrow the scope of the subpoena or withdraw it.

In situations where subpoenas are not available due to statutory limitations, US authorities can be authorized to obtain a formal warrant, which has traditionally required a court order, probable cause and other conditions to be met, and is therefore more difficult to obtain for US authorities. But recent legislation and government practices are believed to have weakened the protections previously afforded by warrant requirements, as further discussed in this memo.

Digital Due Process Coalition and demands to limit access

A number of US-based data hosting service providers and other organizations, including Google Inc., Microsoft Corporation, AT&T, and Ebay formed the Digital Due Process Coalition, which asserts that technological advances have outpaced the *ECPA*, and thus “the vast amount of personal information generated by today’s digital communication services may no longer be adequately protected.” This organization and various privacy activist groups demand that access to personal data (hosted by data hosting service providers and other companies) by US government authorities be limited. Demands include that the situations where US government authorities need warrants be expanded, that warrants should not be – or be less often – available without court orders, that additional limitations should be imposed to legitimize subpoenas (e.g., by enacting new statutory restrictions or interpreting the US constitution to protect privacy interests), that electronic documents stored in the “cloud” be afforded the same Fourth Amendment privacy protections as electronic documents stored in traditional formats, and that consistent standards be set forth for government access to electronically stored information.

Unless and until such reforms pass, the investigative powers of the US government are limited primarily by the following constitutional principles and laws.

Australian Comparison

There is no similar industry lobbying to tighten privacy laws in this way in Australia, nor coordination with local privacy advocates. The previous Australian government was pursuing a policy of compulsory general data retention by carriers and service providers with a view to making archived information available to law enforcement authorities; this would add to recent changes obliging ISPs to retain certain traffic data on specific request. This policy was opposed by industry, but returned to active consideration as the 2012 ‘Data Retention’ proposals.

The Australian *Privacy Act 1988* permits a local company to provide personal information to regulatory authorities without legal compulsion if this is disclosed in the Privacy Policy of the company. Some Privacy Policies state that personal information will not be disclosed to regulatory authorities or other third parties without legal compulsion. In some cases however the concept of ‘implied consent’ has been used to justify such provision.

There are currently few Australian statutory restrictions or conditions on the offshore transfer of data which may become subject to such access. Contractual protections are also of limited value in the circumstances discussed above, especially to data subjects.

Privacy law reform for transferors to generally “remain responsible” after offshore transfer may be of limited benefit to local data owners or individuals once personal data is disclosed as a result of foreign government or litigant compulsion or effective request.

There has, not surprisingly, been recent interest in whether more restrictive oversight of transfer of personal data overseas will be needed in order to bolster the responsibility of transferors. For instance, Senator Stephen Fielding (an independent, though with potential balance of power in the Senate at the time) introduced the *Keeping Jobs from Going Offshore (Protection of Personal Information) Bill* in 2009, which would have required companies to gain customers’ written consent before their personal information could be transferred offshore.

The 2012 amendments to the *Privacy Act*, while not requiring explicit consent, appear more likely to impose liability on Australian hosts for data breaches which occur offshore in some circumstances. . (See also the Privacy Alerts bill of 2013, which may impose reporting obligations.)

Limitations on Searches and Seizures under the Fourth Amendment of the US Constitution

Generally, the primary limit on the US government’s power to obtain personal information is the Fourth Amendment of the US *Constitution*, which prohibits “unreasonable searches and seizures.” Under the Fourth Amendment, the government must obtain a warrant supported by probable cause that a crime has been committed, that describes the “place to be searched and the persons or things to be seized,” and provides simultaneous notice of the search to the person. Whether a search and seizure is “reasonable” depends on whether the person has an objective “reasonable expectation of privacy” in the item subject to the search.

The protection afforded by the Fourth Amendment, however, is not absolute, and there are many exceptions to the warrant requirement.

One such exception is for data held by a third party. Under this “Third Party Exception,” a person does not have a reasonable expectation of privacy in information he or she discloses to a third party. For example, the government does not need a warrant to seize documents that a person conveys to his or her bank (*e.g.* cheques). Similarly, the government does not need a warrant to use “pen registers” and “trap and trace” devices, to record out-going and in-coming call information, because information about the number dialled and the time and duration of the call is accessible to third parties, mainly the telecommunications company.

In the context of electronically stored data, the US government has routinely relied on this Third Party Exception to dispense with the warrant requirement. Federal courts take the view that a person does not have a reasonable expectation of privacy in the subscriber information that he or she provides to an Internet service provider. Therefore, the government was able to obtain the following personal information without a warrant:

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;
2. the information on an individual’s computer that was accessible by a peer-to-peer file sharing program;

3. the chat account information from Yahoo! of a person who used Yahoo's Internet services to access chat boards;
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; and
5. the contents of an iTunes files library shared over an unsecured wireless network.

At least one court took a different approach and held that whether a person has a reasonable expectation of privacy in subscriber information provided to an ISP depends in part on the ISP's terms of service.

Australian comparison

The Australian *Constitution* does not have any provision comparable to the Fourth Amendment to the US *Constitution* which would put limits on Parliament's ability to pass search and seizure laws.

Generally, Australian search and seizure laws can be enforced subject only to the process and limitations, typically about procedure and justification or lack thereof, expressed in the relevant legislation itself – legislation which can be amended, such as during the recent 'war on terror' when certain longstanding common law protections were diluted to some extent.

The *Telecommunications Act 1997* for instance, discussed below, mentions but does not mandate warrants for s313(3) law enforcement help; reports suggest substantial collection of communications traffic data without warrants, including under the *Telecommunications (Interception and Access) Act 1979* (Cth). "Doing your best" for 313(1) crime prevention purposes does not mention warrants; its proper ambit is unclear and seems unlikely to be tested.

The *Privacy Act 1988* may offer some procedural protections, although exceptions permit certain uses and disclosures for law enforcement and related purposes. These bypass questions of 'reasonable expectation of privacy' with simple statutory exceptions, and the Privacy Commissioner's policy *Guidelines* to their use. A recent statement from the Privacy Commissioner in response to questions raised by reports of NSA programs in the US indicates a wide interpretation of the effect of obligations under domestic or foreign law enforcement laws in limiting protections under the *Privacy Act*; in the absence of determinations, this is also unlikely to be tested.

USA Patriot Act of 2001

Following the terrorist acts of September 11 2001, the Bush administration enacted the *USA Patriot Act* of 2001 to expand government powers to obtain data for investigations related to international terrorism and other foreign intelligence matters.

Essentially, this Act had the effect of lowering previous thresholds for the activation of these powers in existing pieces of legislation by amending (a) the *Foreign Intelligence Surveillance Act* of 1978, and (b) other legislation governing National Security Letters. These controversial powers are discussed below.

Privacy and library groups also oppose the "library records request" provision of the *Patriot Act* on the grounds that it "leaves open the door for governmental misuse to broadly investigate library and bookstore patron reading habits."

A reality check asking "who cares" may be appropriate at this point.

Many business operations think it irrelevant if a government wants to check their data in order to fight terrorism, provided the data isn't damaged, lost, misused, or disclosed to competitors. So who would care?

- ❖ Governments typically do not want some of their information, of many types, to be accessible by other governments as a matter of principle, national security or sovereignty.
- ❖ Some businesses (say, a major miner) do not want their information to be accessible to the sovereign wealth funds (for example) of foreign powers.
- ❖ Other businesses may have specific reasons to be cautious about exposure to access, particularly if there is any suggestion of improper or overbroad access to or use of data beyond the purposes for these laws were put in place.
- ❖ Some entities may be willing to accept the initial access but remain concerned about further provision of data to other countries once it has been accessed under this method, due to the operation of other international instruments and agreements.

In any case, it may be harder for, say the US government to find information about an Australian entity hosted in a US data centre than it is to access or discover this information via a request from the US to Australia under various cooperation arrangements (below), and the operation of Australian law in response. Such options would limit the practical need to resort to this method.

Australian comparison

Following the Bali Bombings in 2002, Australia adopted a *National Counter-Terrorist Plan* (2003) and made extensive amendments to surveillance and access powers available to Government authorities.

These have somewhat less impact than the *USA Patriot Act* for our purposes, as they don't introduce administrative subpoenas *per se*, although there were considerable dilutions of existing protections, some comparable with US changes, and investigators gained extended powers and more streamlined procedures.

In subsequent years further legislative changes have somewhat further reduced the difference between thresholds in the US and Australia, and Australia's accession to the CoE Cybercrime Convention in 2012 requires enhanced cooperation with signatories, including the US, although this may make little practical difference – see below.

Foreign Intelligence Surveillance Act of 1978 (FISA)

The *US Foreign Intelligence Surveillance Act* sets out a specific legal framework for surveillance operations conducted as part of investigations related to international terrorism and other foreign intelligence matters. With the introduction of the *Patriot Act*, the *FISA* was amended so that it now applies where a "significant" purpose of a surveillance operation is to obtain intelligence for the purposes of such investigations, rather than the "sole" or "primary" purpose, as it originally stipulated.

The *Foreign Intelligence Surveillance Act* framework will be activated where there is probable cause that the target of surveillance operations is, or is an agent of, a foreign power. Due to the *Patriot Act* amendments, terrorism is now included within the definition of "foreign power", and there is no requirement that targets of surveillance be engaged in any kind of criminal

conduct. In addition, warrants for surveillance operations are issued by the Foreign Intelligence Surveillance Court (FISC), a closed forum separate from the standard federal court system.

Specific powers of law enforcement agencies under the *FISA* (as amended by the *Patriot Act*, *Protect America Act of 2007*, the *FISA Amendment Act of 2008*, and reconfirmed in late 2012) that may constitute potential risks for those hosting data in the US include:

1. The power of the Federal Bureau of Investigation (FBI) to compel the production of any “tangible thing” for the purposes of an investigation to either obtain foreign intelligence or protect against terrorism or clandestine intelligence activities. The FBI may do so by certifying to an FISC judge that the investigation falls within the bounds of the *FISA* and the judge does not have any discretion to refuse the order if certain procedural requirements are met. Persons against whom such an order is made and/or sought are forbidden from disclosing these facts to any other person except for the purposes of complying with an order and/or seeking legal advice.
2. The power to conduct secret physical searches of personal property for investigations in which foreign intelligence gathering is a significant purpose. The person whose property is searched need not be directly involved and the search may be conducted without a warrant, provided that the Attorney General certifies that there is no substantial likelihood the search will involve the premises, information, material, or property of a US person. Subjects of a special search must not be informed of the fact that it has been or will be conducted, and third parties directed to assist must protect its secrecy.
3. The power to obtain a search warrant in all criminal investigations without providing notice to the subject of the search for up to 30 days, or longer upon application to the Court if the facts justify further delay.
4. The power to conduct roving wiretaps on communications lines, which allows for monitoring of several different communications lines across the US. To engage in wiretapping, the government must obtain a warrant from the FISC based upon probable cause that the target is, or is an agent of, a foreign power. Third party communications carriers, landlords and other specified persons must provide access and assistance necessary to carry out the warrant. They must not reveal the fact of the warrant, and must minimize associated disruption to any services they provide to the subject. In the case of third party communications carriers, if a law enforcement authority suspects that the subject of a roving wiretap warrant might use a particular carrier's services, the authority is entitled to monitor all communications transmitted by that carrier. Accordingly, there is a risk that information concerning other clients of the carrier might incidentally be captured.
5. The power of the Department of Justice (DOJ) to grant approval for law enforcement agencies to engage in electronic surveillance without a court order for up to one year for the purposes of obtaining foreign intelligence. There must be no substantial likelihood that a US person is a party to the surveilled communications. Any third party carrier involved in transmitting the communications must assist the surveillance if requested, including by maintaining its secrecy.
6. The power of the federal government to use “pen registers” and “trap and trace” devices to monitor outgoing and incoming phone calls for the purposes of an investigation to gather foreign intelligence information. In some circumstances, relevant communications carriers may be obliged to assist authorities in installing and monitoring such devices, protecting the secrecy of the investigation and minimizing interruption to any services provided to the subject.

In June 2013 the *Washington Post* and *Guardian* published reports of 'data mining' targeting communications of non-US users for national security purposes, with only infrequent high level authorisations, based on broad interpretations of 2008 amendments to FISA. It is unclear the extent to which such programs would affect business-oriented cloud data services. Several major consumer-oriented SaaS providers were reported to have agreed to participate, which could affect 'BYOD' devices, 'ad-hoc' clouds and cloud-enabled PCs, although details of the program and its implications remain in dispute at the time of writing, and some of the allegations have been denied.

'Administrative subpoenas' such as National Security Letters (NSLs)

National Security Letters are a type of federal administrative subpoena by which the FBI may, *without* court approval, compel individuals and businesses to provide a variety of records, including customer information from telephone and Internet service providers, financial institutions and consumer credit companies. An NSL may be issued to any person (even if they are not suspected of engaging in espionage or criminal activity) so long as the issuer believes that they may hold information relevant to a clandestine terrorism or other intelligence investigation. The FBI does not need to specify an individual or group of individuals and each request may seek records concerning many people. For example, nine NSLs in one investigation sought data on 11,100 separate telephone numbers. Moreover, a recipient of an NSL may not reveal its contents or even its existence.

A communications carrier subject to a National Security Letter may be obliged to hand over information about a particular customer, their toll billing records and/or their electronic communications transaction records to the FBI. However, there is no provision requiring a carrier to give the FBI access to the actual content of a client's communications.

National Security Letters have been the subject of considerable legal and political controversy. For example, a number of mandatory non-disclosure clauses have been ruled unconstitutional (and subsequently re-enacted in a different form), and several reports by the US Inspector General have revealed widespread inappropriate use and underreporting by the FBI.

(In March 2013, Judge Susan Illston of the Northern District of California declared, in a case involving the EFF, that 18 U.S.C. § 2709 and parts of 18 U.S.C. § 3511 were unconstitutional. She held that the statute's gag provision failed to incorporate necessary First Amendment procedural requirements designed to prevent the imposition of illegal prior restraints, and that the statute was unseverable and that the entire statute, also including the underlying power to obtain customer records, was unenforceable. The order was stayed subject to appeal. While it could rein in the NSL model of access to network and cloud data to some extent, it remains to be seen whether this ruling survives appeal; or if it does, whether similar replacement provisions will be immediately re-enacted, resulting in minimal effective change.)

Australian comparison

There is no direct equivalent of FISA and the very broad NSL administrative subpoena in Australia.

Certain provisions of recent anti-terrorism laws do restrict the capacity of those investigated to communicate this fact to their associates, but in relation to a limited range of specific offences. Certain provisions of the *Telecommunications Act 1997* (Cth) and *Telecommunications (Interception and Access) Act 1979*, above, refer to national security purposes.

It is unclear what the impact of proposals for increased 'Data Retention' of telecommunications metadata would have if implemented, as no draft legislation was provided by mid-2013. It is expected they would oblige increased retention so that formal court orders could later be made for access to message contents, without necessarily diluting whatever existing requirements for such orders may be in place..

The SWIFT case

A prominent example of the US government's use of an administrative subpoena is the SWIFT case. SWIFT (Society for Worldwide Interbank Financial Telecommunication) is a Belgian-based co-operative active in the processing of financial messages, with about 8,000 banks as members. On average it processed 12 million messages a day in 2005. SWIFT operates two primary data centres, a EU site reportedly in Belgium and a mirror site in the US. After the terrorist attacks of September 11, 2001, the United States Department of Treasury (UST) addressed multiple administrative subpoenas to the SWIFT operations centre in the US under the "Terrorist Finance Tracking Program", requesting a copy of all the transactions in SWIFT's database, rather than just the records of individuals who were the specific targets of the government's investigation. SWIFT complied with the procedures by negotiating an arrangement whereby it transferred data from the mirrored SWIFT database to a "black box" owned by the US enabling the UST to perform focused searches over an extended period of time.

In late November 2006 the EU Article 29 Working Party (the independent advisory body to the European Commission on data protection and privacy) issued an opinion on the processing of personal data by SWIFT concluding that SWIFT and the financial institutions which use SWIFT's services had breached Community data protection law as set out in Directive 95/46/EC, including the transfer of personal data to the United States without ensuring adequate protection and failure to inform data subjects about the way in which their personal data were being processed.

When this controversy developed in Europe, Australia and elsewhere in 2006 after the extent of UST searches over the transactions of European and other citizens became known, European data protection commissioners were ultimately unable to effectively intervene.

Although SWIFT itself is believed to have privately negotiated some constraints on the scope of searches over EU citizen transactions by US agents, SWIFT later formalised ostensible compliance with EU law by joining the US 'Safe Harbor' scheme. (The 'Safe Harbor' is a specific type of 'Adequacy Decision' adopted by decision of 26 July 2000 by the EC to allow the free flow of personal data between the EU and the US, in accordance with the EU Directive 95/46/EC.) This allows limitations on its data protection principles for important public purposes "to the extent necessary to meet national security, public interest or law enforcement requirements".

The episode confirmed the limited options available to foreign data owners in the event of use of such administrative subpoenas.

Electronic Communications Privacy Act of 1986 (ECPA)

The *ECPA* is one of the primary federal statutes protecting the privacy of electronic communications in the US. Within the *ECPA* are the *Wiretap Act*, which prohibits the interception, use or disclosure of wire and electronic communications, and the *Stored*

Communications Act (SCA), which regulates access to stored electronic communications. Consumer groups, privacy advocates and companies, including Microsoft Corporation, Google Inc. and E-Bay (the Digital Due Process Coalition) have criticized the *ECPA* as ineffective in protecting privacy in light of technological changes and are calling for the reform of the *SCA*.

The *Stored Communications Act* provisions at issue provide that the government needs to obtain a search warrant to gain access to the contents of an email that is 180 days old or less but can compel a service provider to disclose the contents of an email that is older than 180 days with only a subpoena.

Critics contend that the widespread use of email and other documents stored in the cloud are increasingly replacing the traditional ways of storing documents in paper form, on a hard drive or on a CD. They point out that information stored in traditional formats would be fully protected by the Fourth Amendment's warrant requirement, yet under the *ECPA*, "an email or electronic document could be subject to multiple legal standards in its lifecycle, from the moment it is being typed to the moment it is opened by the recipient or uploaded into a user's "vault" in the cloud, where it might be subject to an entirely different standard." Applying consistent standards is further complicated with regard to "Friend Requests, Status Updates and other forms of communication that are neither one-to-one communications, like email, nor public forum posts."

Consequently, "courts have not been consistent in applying the Fourth Amendment's warrant requirement and the *SCA*'s 180-day protection for communications in electronic storage to e-mail messages stored remotely on service providers' networks", which creates uncertainty for ISP's and other companies who host content with regard to how the *ECPA* applies to material on their systems.

For example, the Eleventh Circuit held that individuals do not have a reasonable expectation of privacy in read e-mail messages stored with an ISP because they "shared" them with the service provider." In contrast, the Ninth Circuit held that an electronic communication service provider who turns over opened and stored text messages without a warrant or a viable exception is liable under the *SCA* for making an access that was not permitted "as a matter of law". To confuse matters more, a panel of the Sixth Circuit held that users have a reasonable expectation of privacy in e-mails, only to have its decision reversed by the Sixth Circuit sitting *en banc* on grounds that the plaintiffs did not have standing to sue, but without addressing the constitutionality of the *SCA* provisions.

As a result of the ambiguity in the law, the Digital Due Process Coalition has proposed the following changes to the *ECPA*:

1. Treat private communications and documents stored online the same as if they were stored at home, and require the government to get a search warrant before compelling a service provider to access and disclose the information.
2. Require the government to get a search warrant before it can track movements through the location of a cell phone or other mobile communications device.
3. To require a service provider to disclose information about communications as they are happening (such as who is calling whom, "to" and "from" information associated with an email that has just been sent or received), the government would first need to demonstrate to a court that the data it seeks is relevant and material to a criminal investigation.
4. A government entity investigating criminal conduct could compel a service provider to disclose identifying information about an entire class of users (such as the identity of all people who accessed a particular web page) only after demonstrating to a court that the information is needed for the investigation.

Australian comparison

There is no broad Australian equivalent of the 'order to disclose' that is available to US federal government agencies.

However, some Australian government agencies possess similar powers under various legislative schemes. For example, the New South Wales Independent Commission Against Corruption may obtain certain information under State surveillance legislation, and CrimTrac is listed as an 'enforcement agency' under the *Telecommunications Interception and Access Act*.

Also note the proposals for 'Data Retention', mentioned above, introduced publicly in 2012 after apparent development for several years. If implemented, these could require retention of communications metadata for periods of two years or more, which would facilitate local access under a subsequent court order.

Section 313 of the *Telecommunications Act 1997* (Cth) contains two relevant provisions which offset the effect of prohibitions on phone tapping etc. under the *Telecommunications (Interception and Access) Act 1979* (Cth). The first is a 'crime prevention' purpose in s313(1) and (2), which requires carriers, carriage service providers and their intermediaries (but probably not cloud data hosts) to "do their best" to prevent their networks and facilities being used to commit an offence under Commonwealth or state law. Without an obligation to do anything, guidance as to who can request or suggest action, compensation for costs under s314, or guidance as to what might be expected, this is difficult to formally enforce, though there is wide scope for informal pressure. It is the basis for recent informal Internet content blocking, with an ASIC IP block request aimed at fraud pages reported to have inadvertently taken 1,200 and 253,000 non-fraud sites offline in two recent instances.

The more significant provision is a more enforceable 'law enforcement' purpose in s313(3) and (4), which requires carriers etc. to give such help as is 'reasonably necessary' to 'officers and authorities' of Commonwealth and states to enforce criminal laws and those with financial penalties in Australia, the criminal laws of 'a foreign country', or to protect national security or public revenue. Carriers and carriage service providers are exempt from liability for good faith cooperation with both these provisions. 'Help' includes interception warrants, stored communications warrants, local or foreign preservation notices under the *Telecommunications (Interception and Access) Act*, and requires financial assistance for costs incurred in s314.

Most of the law enforcement data surveillance and interception activities listed in s313(7) applying to s313(3) and (4) are based on warrants and notices, rather than mere requests. But the provision is not limited to these. And under s312 ACMA can also issue administrative notices, also under an immunity; and the permissible scope for informal pressure to 'do your best' under s313(1) and (2) is largely untested, and perhaps un-testable. The scope of these sections is thus somewhat uncertain, but clearly requires carrier help at least with reasonable law enforcement requests, including assisting enforcement of foreign laws.

Secret Surveillance Programs

After the events of September 11, 2001, the Bush administration engaged in 'warrantless wiretapping' of phone calls of US citizens for national security purposes. Under this secret surveillance program, telecommunication companies such as AT&T, Verizon and BellSouth assisted the National Security Agency in building a massive database of customer phone records.

Once the warrantless surveillance came to light, privacy and civil rights groups brought lawsuits against the participating companies and the Bush administration. In response, the government enacted a law granting legal authority to the government to intercept certain communications without a warrant, immunity from liability to companies that assist the government with future warrantless surveillance, and retroactive immunity from liability to companies that already participated in the warrantless surveillance program.

Other secret surveillance programs, which were ultimately abandoned, include the 'Total Information Awareness' project, which was designed to detect terrorists by scanning large amounts of consumer data, and the 'Computer Assisted Passenger Pre-Screening System', under which the Homeland Security Department proposed to use information from various databases to classify airline passengers according to their level of risk.

More recent discussions in June 2013 about the scope and oversight of NSA's programs, above, were marked by difficulties experienced by members of Congress, the Senate and cloud business leaders as a result of the secrecy obligations applying to those with official knowledge.

Australian Comparison

There have been no known similar instances in Australia of projects of this magnitude.

In 2012 proposals were advanced by law enforcement and Attorney Generals Department sources for an extensive 'Data Retention' program, above. Although details and justifications of the proposal, which was mentioned briefly buried amongst a range of other suggestions, are scarce, it involves 24 month or longer retention of metadata and traffic data, though apparently not message content, for a variety of purposes including but not only anti-terrorism efforts. If it were implemented in full, it would represent a significant extension of secret surveillance programs in Australia. It is at the time of writing (mid 2013) unclear if this will be the case.

As the interactivity of the Internet and web develops, mere metadata has been said to offer increasing information about the content of messages, arguably diluting the distinction between message content and metadata.

If it were implemented in full, this program may represent a significant extension of secret surveillance programs in Australia, although oversight mechanisms are as yet unclear.

Data Access Demands in Litigation

The US federal government has a broad range of mechanisms to compel production of information in criminal and civil litigation proceedings, including discovery, administrative subpoenas, grand jury subpoenas and court orders.

Rule 34 of the U.S. *Federal Rules of Civil Procedure* imposes a legal duty on companies to retain all documents that may be relevant to pending and reasonably foreseeable litigation. During the discovery process in litigation proceedings, companies must search and produce all relevant records, including electronically stored information. As a result, many companies have implemented systems that automatically scan and copy all electronic records, and users may not even realize that their documents are being stored for future document production purposes.

Australian Comparison

Similar rules apply in Australia.

However, as noted above, there are risks inherent in having data overseas in that, even where same rules apply, the costs of legal action, enforceability of remedies, and investigation or monitoring of developments are all more problematic in another jurisdiction since a local entity will often not have any presence there, and will not be familiar with the requirements for an effective action against a determined access-seeker. Retaining and communicating with remote legal advisors and pursuing litigation offshore can also be more expensive and likely to result in worse outcomes.

One question that may ultimately turn on the factual details of a specific operation will be the risk that if data is stored in the US or another jurisdiction, an Australian company could potentially be exposed to legal action there on the basis of there being a sufficient connection with the jurisdiction. While in most cases this connection alone may be too tenuous to support a finding of such jurisdiction, further advice on specific circumstances may be necessary to exclude the risk of exposure to a US lawsuit that might not otherwise have jurisdiction, on the basis that the data (assets) are there.

Rule 26(b)(2)(B) provides a limited defence to production of electronically stored data “from not reasonably accessible sources, due to undue burden and cost” but there is not much guidance as to what constitutes sufficient “undue burden and cost.” In addition, the party requesting the documents may still obtain limited discovery to test whether the information is truly “not reasonably accessible.”

The government may also issue subpoenas to require private companies to disclose information. For example, the Department of Justice issued a subpoena to Google Inc. to supply a log of random searches made on Google and Internet addresses as part of an unrelated lawsuit involving the *Child Online Protection Act*. The federal judge ultimately denied the DOJ’s request for 5,000 random searches made on Google but ordered Google to surrender 50,000 random Internet addresses. Yahoo! Inc., Microsoft Corp.’s MSN, and America Online Inc., on the other hand, complied with the DOJ’s request for both searches and addresses to varying degrees.

The SWIFT case above is an example of the use of administrative subpoenas in matters which commence as investigations but may ultimately result in litigation to prosecute offences.

Finally, although the disclosure obligations in US litigation may in some cases potentially conflict with foreign data protection laws, such privacy laws of other countries are generally no defence to the legal obligations of entities to comply with subpoenas, warrants and orders that are lawfully issued and served within the jurisdiction of US courts. In the context of such a conflict between US and foreign law, one court put it this way: “The jurisdiction of American courts is unquestioned when they order their own nationals to produce documents located within this country” (*i.e.* the foreign law is not a relevant consideration).

Access Requests on Behalf of Foreign Governments in Connection with International Assistance

The U.S. has entered into mutual legal assistance treaties with over 50 countries, as well as a mutual legal assistance agreement with the EU. The cooperation under mutual legal assistance

arrangements can include substantial sharing of electronic information between law enforcement authorities in the two countries.

For example, in 2006, the US ratified the Council of Europe *Convention on Cybercrime*. This Convention provides for gathering and sharing electronic data and evidence at the request of foreign law enforcement agencies, including:

1. expedited preservation of stored computer data, pending a request for search, seizure or disclosure of data,
2. expedited disclosure of traffic data, when the execution of a request to preserve traffic data indicates that another country was involved in the transmission of the communication,
3. search, seizure and disclosure of stored data,
4. real-time collection of traffic data, and
5. interception of the content of specified communications.

They also include an invitation to spontaneously offer data to a foreign state.

In addition, the *Additional Protocol* of 2003 makes publication of racist and xenophobic propaganda via computer networks a criminal offence. This may have impact on systems open to a large local user population.

Companies storing data in the US, therefore, may be subject to requests for data from foreign governments.

Australian comparison

The *Mutual Legal Assistance Treaty* (Treaty) between the United States and Australia came into force 30 September 1999. This provided a bilateral mechanism where foreign law enforcement agencies can obtain access to data posted in other jurisdictions subject to control or supervision by the foreign government.

The Council of Europe *Convention on Cybercrime* was ratified in 2012 by Australia. Key provisions of this convention are set out above, mostly those in Chapter III, Articles 23 and 25, including expedited search, seizure and real-time interception of content.

Australian ratification of the *Convention* will mostly build on the *Mutual Legal Assistance Treaty* as between Australia and the US, and thus may have little additional impact on the exposure of Australian-owned data held in the US to access by other foreign governments (since this is already facilitated by US ratification of the *Convention*, and to some extent the operation of the *Treaty*). However it will clearly increase the exposure of Australian data held in a European 'cloud' to access from other signatories, including those in the US.

(It should be noted that recent reports of plans for European Cloud services with components tied to national borders suggest they may have come about in response to the increased exposure to *USA Patriot Act* requests. It will be interesting to assess the degree to which these initiatives may offer guidance for Australian adaptation to the new environment.)

Analysis

When data is hosted overseas, it is subject to the law of the jurisdiction where it is held. Direct local access to data by the host country obviates the traditional process of disclosure and cooperation between national law enforcement agencies. The data is also subject to access under the civil process of the foreign nation.

This will have different implications depending on the nature of the law of the host jurisdiction and, to some extent, the relationship between Australia and the government of that nation.

In considering the case of cloud data hosted in the United States, the differences between the legal environment in Australia and the legal environment in United States are many and extensive. Although the policy objectives and practical effect of government agency powers are roughly comparable, it is clear that American law is focused on the protection of the US national interest. It may be also inherently more difficult for companies or individuals based in Australia to monitor, assess and if necessary seek to restrain the conduct of search, interception or surveillance activities by governments or litigators of a foreign jurisdiction. In addition, the scale of surveillance activity undertaken in the United States, and consequent concerns expressed by industry regarding the extent of expanding government powers, have not emerged in Australia to the same degree.

When the conduct of SWIFT in making its data available to the UST became public knowledge the European Parliament, echoed by some local commentators, declared that it was deeply concerned about the purposes of the transfer of data to the UST, the lack of the procedural protections expected in the source countries, and that such operations were taking place without “the citizens of Europe and their parliamentary representation having been informed.”

While the potential for counterproductive “digital protectionism” deserves investigation, such concerns with US access to European data hosted on US Cloud services appear to have ongoing effect on plans to implement services which assert European countries’ data sovereignty.

In our view, while the picture is complex, the concerns expressed by the European Parliament are concerns should resonate with Australian customers considering hosting data in or under jurisdictions such as the United States and elsewhere, and give rise to caution regarding the nature of the information to be transferred, the potential interests of the data owners in relation to that information, and increased needs to fully understand (and, more concretely, disclose to the data owner) the characteristics of the foreign legal environment.

[Some print versions of this report are simplified by omission of the notes and references in the full version. Please retrieve the online version to follow up our sources.
See inside cover for details.]

6. Security Considerations

Cloud services, with their massive ‘honeypots’ of tempting personal and business data, pose a serious challenge for IT security protection whether onshore or off, but also offer platforms for potentially meeting those threats in certain circumstances more effectively than non-cloud systems.

This chapter briefly touches on the recent history of cloud data breaches, flags two key issues to address, and offers an example from the DSD in the form of a checklist, with cloud specific issues flagged.

Never-ending Stories of Data Breaches Focus the Mind on Security

Ensuring a customer can manage their information in the cloud is important because data breaches are common. In 2010/2011 the Office of the Australian Information Commissioner (OAIC) was notified of 56 data breaches, under its voluntary notification scheme, and investigated a further 59 which were not reported, in 2010/2011. US figures indicate that some 88% of organisations have at least one data breach each year.

High profile data breaches illustrate how easy it is to lose control over information, especially when the information is held on computers. Examples include recent hacking of Twitter accounts [insert]. Hacking of Sony’s servers when hackers obtained account information, including credit card information, relating to some 100 million users. In 2011 hackers also accessed Citigroup’s online system, compromising account data such as names, contact details and account numbers of some 360,000 customers. Also in 2011, Australian webhosting provider DistributeIT confirmed that hacker activity resulted in the permanent loss of data from some 4800 customer websites. In July 2012 hackers accessed hosting provider MelbourneIT’s servers deliberately targeting MelbourneIT’s customer telecommunications company AAPT’s data as a protest against proposed new laws requiring telecommunication companies to keep call records for two years. Confidential information of AAPT clients was published.

These examples serve to confirm that complacency is not warranted, and that planning must assume a high likelihood that a data breach may occur and thus seek to minimise their impact. (See the end of this chapter for a reference to the proposed new mandatory disclosure breach notification ‘Privacy Alerts’ law introduced as we go to press.)

Two key IT security issues for the cloud

The two key security issues that arise when an organisation or business considers whether or not to store digital documents in any cloud service are:

- ❖ How can the digital documents best be protected from unintended access or loss as a result of their cloud connection? (i.e. How can you make them as safe as reasonably possible?)
- ❖ If there is a ‘data breach’, how will responsibility for the security breakdown be allocated? (i.e. How can those best placed to resolve the risk carry some of the cost?)

Cloud Computing Security Considerations – Checklist (DSD)

This non-exhaustive list of cloud computing security considerations is from section 17 of the Defence Signals Directorate/Cybersecurity Operations Centre, *Cloud Computing Security Considerations*, with cross-references to other paragraphs for more information.

“Placing a cross instead of a tick beside any of the following security considerations does not necessarily mean that cloud computing cannot be used, it simply means that the security consideration requires additional contemplation to determine if the associated risk is acceptable.”

While companies and individuals may have a somewhat lower sensitivity to certain IT risks than some government agencies (the primary audience for this list), and hence some considerations may not apply, these considerations do offer a useful starting point for analysing the degree to which Cloud contracts, and the services provided under them, can address wider business and other security risks.

[*An asterisk and bold text, added by the authors here, tags items that are particularly relevant to data sovereignty questions.]

- ❖ *** My data or functionality to be moved to the cloud is not business critical (19a).**
- ❖ I have reviewed the vendor’s business continuity and disaster recovery plan (19b).
- ❖ I will maintain an up to date backup copy of my data (19c).
- ❖ My data or business functionality will be replicated with a second vendor (19d).
- ❖ The network connection between the vendor’s network and me is adequate (19e).
- ❖ The Service Level Agreement (SLA) guarantees adequate system availability (19f).
- ❖ Scheduled outages are acceptable both in duration and time of day (19g).
- ❖ Scheduled outages affect the guaranteed percentage of system availability (19h).
- ❖ I would receive adequate compensation for a breach of the SLA or contract (19i).
- ❖ Redundancy mechanisms and offsite backups prevent data corruption or loss (19j).
- ❖ If I accidentally delete a file or other data, the vendor can quickly restore it (19k).
- ❖ I can increase my use of the vendor’s computing resources at short notice (19l).
- ❖ I can easily move my data to another vendor or in house (19m).
- ❖ I can easily move my standardised application to another vendor or in-house (19m).
- ❖ My choice of cloud sharing model aligns with my risk tolerance (20a).
- ❖ *** My data is not too sensitive to store or process in the cloud (20b).**
- ❖ *** I can meet the legislative obligations to protect and manage my data (20c).**
- ❖ *** I know and accept the privacy laws of countries that have access to my data (20d).**
- ❖ *** Strong encryption approved by DSD protects my sensitive data at all times (20e).**
- ❖ The vendor suitably sanitises storage media storing my data at its end of life (20f).
- ❖ The vendor securely monitors the computers that store or process my data (20g).
- ❖ I can use my existing tools to monitor my use of the vendor’s services (20h).
- ❖ *** I retain legal ownership of my data (20i)**
- ❖ The vendor has a secure gateway environment (20j).

- ❖ The vendor's gateway is certified by an authoritative third party (20k).
- ❖ The vendor provides a suitable email content filtering capability (20l).
- ❖ The vendor's security posture is supported by policies and processes (20m).
- ❖ The vendor's security posture is supported by direct technical controls (20n).
- ❖ I can audit the vendor's security or access reputable third party audit reports (20o).
- ❖ The vendor supports the identity and access management system that I use (20p).
- ❖ Users access and store sensitive data only via trusted operating environments (20q).
- ❖ The vendor uses endorsed physical security products and devices (20r).
- ❖ The vendor's procurement process for software and hardware is trustworthy (20s).
- ❖ The vendor adequately separates me and my data from other customers (21a).
- ❖ *** Using the vendor's cloud does not weaken my network security posture** (21b).
- ❖ I have the option of using computers that are dedicated to my exclusive use (21c).
- ❖ When I delete my data, the storage media is sanitised before being reused (21d).
- ❖ *** The vendor does not know the password or key used to decrypt my data** (22a).
- ❖ The vendor performs appropriate personnel vetting and employment checks (22b).
- ❖ Actions performed by the vendor's employees are logged and reviewed (22c).
- ❖ Visitors to the vendor's data centres are positively identified and escorted (22d).
- ❖ Vendor data centres have cable management practices to identify tampering (22e).
- ❖ Vendor security considerations apply equally to the vendor's subcontractors (22f).
- ❖ The vendor is contactable and provides timely responses and support (23a).
- ❖ I have reviewed the vendor's security incident response plan (23b).
- ❖ The vendor's employees are trained to detect and handle security incidents (23c).
- ❖ The vendor will notify me of security incidents (23d).
- ❖ The vendor will assist me with security investigations and legal discovery (23e).
- ❖ I can access audit logs and other evidence to perform a forensic investigation (23f).
- ❖ I receive adequate compensation for a security breach caused by the vendor (23g).
- ❖ Storage media storing sensitive data can be adequately sanitised (23h)."

In particular, 'Protecting Data from Unauthorised Access by a Third Party' flags two critical issues for data sovereignty:

Legislative obligations. What obligations do I have to protect and manage my data under various legislation, for example the *Privacy Act 1988*, the *Archives Act 1983*, as well as other legislation specific to the type of data? Will the vendor contractually accept adhering to these obligations to help me ensure that the obligations are met to the satisfaction of the Australian Government?

Countries with access to my data. In which countries is my data stored, backed up and processed? Which foreign countries does my data transit? In which countries is the failover or redundant data centres? Will the vendor notify me if the answers to these questions change? Data stored in, processed in, or transiting foreign countries may be subject to their laws. Such laws range from Freedom of Information requests by members of the public, through to government lawful access mechanisms.

For example, a foreign owned vendor may be subject to their country's laws even if the vendor is operating within Australia. If the vendor is subpoenaed by a foreign law enforcement agency for access to data belonging to the vendor's customers, the vendor may be legally prohibited from notifying their customers of the subpoena.

These two issues may explain why DSD recommends against outsourcing information technology services and functions outside of Australia, unless agencies are dealing with data that is all publicly available:

"DSD strongly encourages agencies to choose either a locally owned vendor or a foreign owned vendor that is located in Australia and stores, processes and manages sensitive data only within Australian borders. Note that foreign owned vendors operating in Australia may be subject to foreign laws such as a foreign government's lawful access to data held by the vendor."

Cloud security more generally

As always, it is also critical to remember that one difficulty with IT security is the 'unknown unknowns' that 'business as usual' compliance-centred models may fail to prepare for and mitigate. With IT security threat evolution currently more than keeping pace with remedial IT security measures, and new business models and threats emerging constantly, a key challenge is how to explore for such novel and unpredictable risks while pursuing sensible compliance and procedural remedies addressing more established and well understood threats.

A full exploration of Cloud security issues is beyond the scope of this paper, and will no doubt remain the subject of attention from a significant part of the IT security industry and research sector. The proposed new laws for data breach notification, *Privacy Amendment (Privacy Alerts) Bill 2013*, will likely play a key role in keeping this issue at the forefront of CIO/CTO concerns.

The proposed new laws for Data Breach Notification (*Privacy Amendment (Privacy Alerts) Bill 2013 (Cth)*) will likely play a key role in keeping this issue at the forefront of CIO/CTO concerns.

See the References section at the end of the full version of this paper for a variety of readings which can assist further investigation of cloud security from a technical perspective.

(See also Chapter 3 above, "Risk Management and Governance", for more information on risk assessment.)

[Some print versions of this report are simplified by omission of the notes and references in the full version. Please retrieve the online version to follow up our sources. See inside cover for details.]

7. A Cloud Data Location and Jurisdiction Policy?

Developing internal cloud data location and jurisdiction policies

A cloud data location and control policy should seek to completely and faithfully automate the entire life cycle of all networked data within a company, from their creation to destruction.

It answers questions about whether there is any data which must be, or should be held in a particular location or under the control of entities regulated by a particular jurisdiction, and if so, how to respond to this need.

Once an organisation establishes a means for the creation of a cloud data location and jurisdiction policy, they must begin by addressing key issues that form the substantive basis of the policy.

What is the Company's Regulatory Environment?

The committee must identify the regulatory environment that the organization operates in, for instance:

- ❖ What statutes and case law directly affect the company?
- ❖ What codes, standards and/or rules of professional practice are the company obliged to follow?
- ❖ What codes, standards and/or rules of practices could the company choose to further comply with?
- ❖ What jurisdictions can affect the data, either through its location or the entities that control it?

Key factors affecting your Cloud Data Location and Jurisdiction Policy

The committee must simultaneously develop a firm-wide digital document policy that will orchestrate how all the regulatory factors are to be dealt with. Key considerations to be kept in mind are:

- ❖ The nature of the data, and whether there are particular legal, regulatory or similar obligations favour certain locations or jurisdictions
- ❖ The characteristics of your customers, staff or partners: are there particular expectations or vulnerabilities to take into account?
- ❖ Risks associated with exposure to various jurisdictions, especially the attitudes and practices of entities who may be seeking access to the data

What are cloud data location and jurisdiction policy benefits?

After implementation of the policy, several benefits should potentially flow to the company, for instance:

- ❖ Improvements in decision making processes;
- ❖ Reduced specification and investigation costs for individual projects;
- ❖ Reduced reliance on local storage requirements and associated costs, since only those data sets necessary to retain in a certain jurisdiction will be handled this way,

while others may be treated in a more economical manner;

- ❖ A streamlining of the compliance process with statutes, rules and standards;
- ❖ An ability to guarantee the location, control, security and integrity of data;
- ❖ The ability to locate, and assure the entire life cycle of, all critical data required for legal purposes;
- ❖ Reduced risk of unexpected or unwanted exposure to litigants or other entities from other jurisdictions
- ❖ Increased awareness of the level of exposure to such entities from all jurisdictions

(Note however that there are some limitations arising from the nature of cloud services, and cloud providers. It is almost never possible to do an inspection or audit of a cloud service facility. Whether or not a contract can be negotiated depends on the scale of the business and the extent to which it is a bespoke service; many of the lower cost service contracts are unilateral and non-negotiable. More important is the cap on liability and provisions requiring positive disclosure, indemnity and assistance in case of data breach. See Chapter 3 above for more detail on some of these aspects.)

Who else should be responsible for digital document location and jurisdiction policies?

Once all aspects of the regulatory environment have been itemised and readied for specific attention in accordance with the control policy, the next task is the committee's assigning of responsibility for protocols and various regulatory items. Regulatory items affecting the company must be apportioned appropriately between executives, record management professionals, system administrators and other staff.

Records managers: Internal records managers should be tasked to design, develop and implement the networked data storage system and required protocols, in co-ordination with system administrators. It is advisable to pilot, test and refine such systems and protocols with actual users and support staff prior to enterprise-scale rollout.

Supporting infrastructure: In turn, systems administrators must be tasked to have in place hardware and processes that insure all cloud data is where it should be at any given time, including after inevitable changes to IT. IT managers should be made aware of the various evidentiary and long term data production requirements, including those related to other jurisdictions, and asked to explicitly address technical obsolescence of data storage tools, and meta data features which offer benefits for implementing data jurisdiction or location policies.

Training: All employees must undergo training to inform them about the cloud data system and processes, the regulatory environment that requires a policy, the responsibilities they must adopt to directly assist with observance of the policy, and particularly how each employee's specific duties affect the proper observance of the policy, right down to discrete items such as local and BYOD cloud tools infiltrating all aspects of the IT environment. (This may also be a good time to make sure there is a sensible and widely understood policy about BYOD and personal device usage.)

Compliance and enforcement: Lastly, senior executives must insure the continued firm-wide adherence with and implementation of the policy, and they must utilise an appropriate reporting system for efficiently communicating with the committee all issues as they arise regarding ongoing adherence and implementation of the policy. Where anomalies or practical difficulties do arise, these should be addressed explicitly (perhaps by variation of the cloud data location or control policy) rather than being seen merely as a compliance problem.

Creating a Policy

So what do you look at for taking concrete steps to deal with the problems revealed above? This section provides sources to properly start the process in the absence of external professional assistance.

Customised: Your specific circumstances should affect the strategic approach and the procedural details of a cloud data location or jurisdiction policy, as simply adopting a generic policy may not be appropriate for your risk profile, technical infrastructure or operational realities, or specific enough to give necessary guidance to users.

Due diligence: Bear in mind that external and internal due diligence investigations may take into account the state of an organisation's network and cloud data management systems and information assets, and also whether the stated policies and actual practices give confidence that appropriate data would be protected from a variety of foreseeable risks. One feature of this inquiry may be the degree to which the unique challenges of cloud data services have been addressed, and the risks of exposure to other jurisdictions realistically assessed.

Standards: Local and international formal standards can establish the foundations for what constitutes standard practice, and should be explicitly taken into account when developing a cloud data location and jurisdiction policy. See the next chapter for more details.

How do you develop a policy to deal with all these issues?

So far we have broadly described the main considerations and issues that a corporation must investigate when formulating a cloud data sovereignty policy.

This section highlights approaches that have been developed and adopted around the world and within Australia. The approaches described below are used by the home government departments in the countries of their creation (and by degrees their private industries and business communities), so most have been tried and tested before being incorporated into governance practice.

A written and effectively distributed internal policy document encompassing both locally networked and remote cloud data can provide strong evidence that a company has legitimately chosen where to locate data by following reasonable and objective standards. Bolstering such a conclusion would be clear evidence of a firm's having reasonably incorporated variously stated domestic and international Standards or Policies.

However the creation of a firm specific data location or jurisdiction policy is no easy feat. To this end the authors suggest that firms consider consulting with data storage and information management professionals, particularly given the ease with which essential issues could be overlooked by a firm, and for the other simple reason that what may appear to be too difficult for a firm to implement, may be readily and affordably solvable by those already possessing years of practical experience in this field.

Guidelines: what should be included?

With the global standardization of IT software and systems, together with what appears to be a judicial determination to standardize a common cross-border jurisprudence towards IT evidentiary issues, it is no longer surprising to find that IT standards in many countries are beginning to reflect one another.

This is of course critical for many aspects of cloud services hosted in other countries, but even services hosted inside the home country may need to take into account such influences.

With the above in mind, the reach of a firm's business beyond its national borders should, we believe, require that a firm at least examine and consider the adoption (partially or otherwise), of standards or policies found outside its home country.

At the very least a cloud data sovereignty policy should seek to strongly reflect any standards or policies already established within a firm's home country.

Australian standards

AGIMO has proposed models for assessing legal issues in cloud contracts. As noted above, DSD has also mapped out security issues for consideration in the cloud in addition to normal IT security matters.

International standards

See ISO 27001, above. (The detailed application of international and foreign national standards is beyond the scope of this Report; the reader is encouraged to investigate sources applicable to jurisdictions and industries of interest.)

Classification of data

A fundamental issue for the policy is to assist the classification of data into categories that have consequences for decisions on location, jurisdiction, acceptable risk and access control.

Criteria These classification criteria will need to be tailored for both operational business needs, and the specific data storage or use obligations revealed by a detailed analysis of the legal and other constraints on your various activities and digital assets (see below).

The classification criteria and policies will need to be checked by a variety of stakeholders and advisers, and refined by trials in practice.

Simplicity The criteria and classification procedures will become embedded into the core processes of the organisation, so they should be as simple and clear as possible while still permitting the various requirements to be met.

Who decides? Substantial effort may be required to establish efficient procedures for the involvement of various people in the classification process. Depending on the nature of the criteria, certain classification decisions may need to be made by more senior staff or even legally qualified advisers, while the bulk of them should be made routinely, either by automated methods or simple choices at the time of creation.

Review Classification does not necessarily occur just once. A routine process of reviewing data sovereignty and location issues, or at least the triggers for such a review, should be described.

This is so that if circumstances change (such as through the onset of a litigation risk, or a fundamental change in a technical process supporting certain types of data storage) certain data can be reviewed for reclassification – otherwise they may be inadvertently hosted inappropriately to new circumstances.

What data is regulated and what is not?

When developing the criteria, it is important to consider detailed analysis of the application of particular provisions of applicable laws in relevant jurisdictions. Data that may on first glance fall into one category may at law belong in another; and where it does fall into a key category, the obligations around it may not be what they first appear. The categories and obligations should be taken into account in developing the criteria.

For instance “Personal information” (under Australian privacy law), “Personal Data” (EU) or “Personally Identifying Information” (US) are similar but not identical concepts for important data sets that nevertheless cover a relatively limited class of business information, and it may be possible to ensure that all information held by a service provider is de-identified (and not easily re-identifiable). In such cases there are no privacy rules applying to the data, since it is outside their scope of “personal information”.

(The ease or difficulty of possible re-identification may affect its characterisation under Australian or EU law; less so under US law.)

There are also longstanding wide exceptions to the coverage of the *Privacy Act* (Cth): small businesses, employee records, information related to corporate customers, and many others.

The revised *Privacy Act* coming into force in 2014 doesn't say that foreign providers must comply with Australian privacy law, only that they must not breach the law in holding Australian data. This may limit the scope of the data to be treated in a certain way.

A recent paper from the US Department of Commerce looks at a similar concept arising from the Safe Harbour arrangements between the US and EU. If the data processor promises to secure the data and hold it strictly at the direction of the data collector, the "will not breach" obligation is satisfied.

Data Accessibility

A *Cloud Data Location and Jurisdiction Policy* needs to explicitly address the issues surrounding data accessibility to various parties, including:

- ❖ technological constraints on accessibility, including formats and obsolescence on various platforms, and interoperability or migration issues
- ❖ backup and archive versions of data, in different locations
- ❖ legal and regulatory constraints on location, jurisdiction and accessibility
- ❖ long term access issues, including when laws or business practices change in cloud host countries, or access regimes change
- ❖ processes for different risk categories of data
- ❖ the approach to determining and changing decisions on these issues.

8. Pulling it All Together

Once the cloud data location and jurisdiction risks are identified and analysed, the obligations for each option are understood, the assessment criteria developed, and procedures trialled, these components can be drawn together and integrated into normal operations.

Interaction with your tools and other policies

The smooth operation of a *Cloud Data Location and Jurisdiction* policy will depend on how well it interacts with and is supported by current and future online tools you use, and with the suite of other IT and data related policies you may have in place.

Implement and integrate

The components of the policy need to be integrated into a master document.

Draft materials for various groups of users may be derived or extracted from this master document and checked and tested in practical trials. All the various work groups affected by with the policy should be involved in these trials, and the assessment of changes likely to be required in their areas.

When you are satisfied that the revised core policies and the associated materials for various user situations have been proven in practice, it's time for rollout and implementation.

This should include a substantial training component at all levels of the organisation, and extra assistance tailoring the policy to specific critical areas.

Audit and evaluation

It is important to design a development, audit and evaluation process to assess and help refine the operation of each part of the policy in each area of work and with each document type.

This audit and evaluation is worth doing both during the initial implementation stage, to fine tune the policy and criteria before they are fully established, and also in a routine mode, to demonstrate things like:

- ❖ The policy is well known, understood and implemented in practice, with a training element and appropriately helpful documentation.
- ❖ All data hosted in the cloud is classified according to the policy, and as far as possible that classification is associated directly with the data to enable automated processing of rules.
- ❖ Backups can actually enable restoration of intended files, wherever held.
- ❖ Archives exist for cloud data, and have been implemented according to the policy, and the risks and classifications in it.
- ❖ Litigation, law enforcement and similar risks have been identified and reviewed, and their relevance to specific cloud data risk profiles and location choices has been taken into account in automated and manual processes.

- ❖ Staff are aware of the nature of risks concerning both enterprise level cloud systems and smaller scale or personal/BYOD utilities.
- ❖ Choices about sovereignty and location of all data types and in all areas of operation occurs subject to the policy and the controls it stipulates.
- ❖ Staff are aware of the hazards of a mix of local and cloud data in a variety of systems, and have rules of thumb for managing these hazards.

In many cases the audit process may merely confirm that you have got it roughly right, but it is important to carry out such an exercise at various times to ensure that the system you set up is viable and operational in all major respects.

Note also that as mentioned above, some of the characteristics of some Cloud contracts or services may prevent complete coverage of all these issues.

As discussed above, it may be too late or too expensive to fix it if failure is revealed only at the onset of an external crisis or litigation.

The audit should be integrated with the audit processes for other aspects of the organisation's activities, but produce a specific report addressing the adequacy and operation of your cloud data location and security policy.

9. It's not too hard!

We started off noting the discomfort that consideration of the complexities of data sovereignty and cloud data management can sometimes cause, and the tempting call of the 'too hard' basket.

We have shown how you can analyse the various technical, legal and business issues in turn, and then develop a range of actions that can both reduce the risk of a cloud data disaster, and at the same time increase the value of your information assets.

Hopefully by now you will have come to the conclusion that it is not all too hard.

Some data may happily be hosted almost anywhere or by anyone, while other data may have features which require consideration of location and jurisdiction. But if you have full visibility of data collection, storage and use processes for other purposes, you may well have most of the information at hand needed to make these decisions and implement them.

You need only go into a little more detail than we have covered here to ensure that the specific circumstances of your situation are properly taken into account along with the general principles we describe. We've mentioned a few of the types of expert assistance that may be of value in such an exercise. Eventually the outcomes of such a review will just be integrated with other IT and operational issues to help refine your standard operating procedure.

The benefits of dealing with these matters properly and in advance outweigh the risks, and in time we expect that this will become just another policy for the modern corporation to use to encourage compliance with best practice and good governance.

Think how glad you will be when you can be assured of who has the capacity to access your data in the cloud – if the data you are looking for has become the subject of dispute, you'll know where it is, and the risk and regulatory framework which put it there.

Hopefully this will bring relief from that nagging concern that there may be a nasty surprise awaiting somewhere in your organisation's tangle of data, servers and outsourced storage functionality – so you can with confidence focus on obtaining the business benefits of the ever-expanding suite of cloud services, without waiting for the surprise that announces all clouds aren't necessarily equal.

Data Sovereignty and the Cloud
A Board and Executive Officer's Guide