The Cloud and Data Sovereignty after Snowden

David Vaile[1]
Co-convenor, Cyberspace Law and Policy Community,
UNSW Faculty of Law

The Snowden revelations have renewed interest in questions surrounding jurisdictional issues about where data is kept (location) and who claims the capacity to direct access to it be given by the entity hosting it (control). While early attitudes to the cluster of technologies marketed as The Cloud generally played down this aspect, and unilateral contracts offered by many major providers declined to specify these parameters for the technical provision of a Cloud service, growing appreciation that assurances of security and confidentiality are no barrier to certain forms of access being granted to third parties in other jurisdictions has rekindled interest. This paper explores the technical and legal issues involved from the perspective of an Australian business interested in both customer and government attitudes, and discusses how moves to implement jurisdiction location and control preferences have been characterised as Data Sovereignty and Digital Protectionism by differing interests.

Contents

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

1. Introduction

> *'Then data sovereignty, privacy and security—the importance of trust. … We conducted a survey [in 2010] of 500 consumers in Australia. … [T]he number one thing was that Australians were the most extreme in their responses [in] five out of six categories compared to any other country in the world. The only country more extreme about the data was Germany.*
> …
>
> *Australians didn't trust the government with their data: only 20 per cent trusted the government. They trust IT companies [even] less than the government. …*
>
> *Australia was the most extreme out of the countries we [surveyed] about keeping data on shore. The data needed to be kept in Australia. So it's not just some rule that APRA's made up or the Privacy Commission's made up. It actually reflects Australian consumers' attitudes to data. They want to keep it here'.* (Baty 2011)

What have become known as the Snowden revelations started in June 2013 with stories in the *Guardian*, *ProPublica*, *Washington Post*, later *New York Times* and *Der Spiegel*, and more recently the new online vehicle *First Look*. The scope of the extracts from a cache of tens or hundreds of thousands of files copied from NSA sources by Edward Snowden is remarkable. They purport to reveal an international network of surveillance practices by members of the Anglophone "Five Eyes" intelligence and national security "community" that extend far beyond popular understandings of the controlled and specific powers to tap telephones for law enforcement purposes dramatized by TV's *The Wire*. Critical attention has focused on what seems to be an omnivorous global dragnet based on warrantless, suspicionless mass surveillance programs with ominous names such as BOUNDLESS INFORMANT, collecting digital metadata and some content data both by the legal means we consider below, and by other technical means that bypass the need for cooperation from the Internet backbones, cloud hosts and telecommunications utilities pressed into service by those legal means.

The revelations have bolstered the need to re-assess issues of 'data sovereignty' in the Cloud (an online service delivery method the technical models for which are set out below). These issues, discussed in this paper, had already been coming to attention in countries around the world, including through scholarly work such as that of Dan Jerker Svantesson (2013) and

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

Christopher Kuner (2010) and attention in EU's Article 29 working party and OECD medical informatics circles, but the frequent absence of concern for the expectations of "non-US persons" in the debates following the exposures have confirmed the need for caution, both in relation to the actual practices revealed, and to the potential for similar hazards in other jurisdictions not similarly exposed, and other business practices in cross-border Cloud services. The time for a more traditional, sober analysis of liabilities, risks and benefits has arrived. The carefree, boundless honeymoon of the Cloud is over.

While the Australian Law Reform Commission and parliamentary committees the mid-2013 developments mean renewed attention in Australia is being directed to issues arising from storage of business and personal data in the Cloud, building on trends already identified in the industry insider Baty's view quoted above, coming to us from a more innocent, pre-Snowden era. We investigated questions such as the following:

- How can Cloud services be used safely, and when can they be dangerous?
- What is 'data sovereignty' in the Cloud? Does anyone know or care about legal jurisdiction over data in the Cloud, or is 'cyberspace' somehow beyond such administrivia, as customers are implicitly invited to imagine by some Cloud proponents?
- 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?

The Australian Communications and Media Authority chair explains data sovereignty as "the ownership of data and access to data stored in countries, other than the one where the end user resides, including relevant redress mechanisms and the capacity of citizens of Australia to take action or seek redress against cloud providers in other jurisdictions" (Chapman 2013).

Many organisations' document or data management policies may not yet adequately cover *data jurisdiction,* the key issues of *where it is located* and *who has the capacity to control it*, nor recognise challenges thrown up by a somewhat chaotic, rapidly-evolving cloud services environment increasingly integrated with 'Big Data' capacities (Mayer-Schonberger & Cukier 2013).

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

Governments and regulators seeking to "drive confidence among businesses and users that cloud service contracts will be designed with relevant risks and benefits that have been appropriately weighted and addressed—'balanced' (Chapman 2013) — may also have to pay more attention to the 'risk' side of the equation in this jurisdictional area. A feature of many Australian Cloud policy and strategy documents[2] appears to be an almost boosterish urge to encourage and foster Cloud take-up for its own sake (no doubt welcome to the ears of cloud providers): identifying the benefits, but tending to leaving the hazards, especially those related to jurisdiction, un-named or relegated to a footnote (DBCDE 2013; AGIMO 2013). Confidence may be better served by a more detached, fine-grained risk/benefit assessment of the match between your own data's sensitivity and needs, and the willingness and capacity of Cloud services to deliver reliably, including the potential effects of where they are located and by whom controlled, and the regulatory regimes that become important when things go wrong.

This paper looks at issues affecting data sovereignty in the cloud, and their implications for managing the potential risks and rewards of handling new cloud services safely. The focus is 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. Some countries play a more central role in the cloud industry than others; we offer international equivalents and comparisons to put the differences and similarities in context.

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." (QMUL 2010)

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.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

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 section 4 below.

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

Particularly for Web-grade IaaS (Infrastructure as a Service; see below for cloud acronyms), service provider business models may rely on excluding liability for matters which may be within their control. Typical SaaS (Software as a Service) host models may also depend escaping liability for such matters.

Some countries or jurisdictions may have worse IT, security or privacy protections for your data than Australia; or their protections may be harder for local 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, although recent developments in aggressive surveillance and associated moves by agencies to undermine cryptographic standards have suggested that it may have paradoxical effects in others, potentially reducing security and confidentiality against the intervention of foreign agencies. Many countries (although probably the minority of major cloud participants) are not a party to relevant agreements; some of them also have quite underdeveloped legal coverage of online issues generally, and may not support a robust confidentiality and privacy regime.

And those who are parties to a Convention may have varying implementations of its model laws, and differences of focus between enforcement and confidentiality. The US and Italy for instance have exposed their citizens to fewer of the more extreme effects of the Convention than has Australia, meaning that rights and obligations may not be symmetrical (differing attitudes to strictness of requirements for dual criminality, or to weakening the need to prove a mental element in certain cybercrime offences are examples).

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

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. This is a major feature of the paper.

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 organisation at risk, but also the personal reputations (or even the civil or criminal liability) of those directors or executives who lead it.

Strategic importance to the organisation: methodical solutions needed

The judicial gaze has begun to focus upon the entire stores of information held by companies, and how companies deal with, and secure or fail to secure, those stores. Governments increasingly require transparency around IT security failures (data breach notification); a version of the 2013 Privacy Alerts bill to amend the *Privacy Act 1988* (Cth) to make such notification mandatory, consistent with expectations in many US and EU jurisdictions, may yet be reintroduced. And every Internet user has been alerted, by the media at least, to the risk of their data being subject to access by unwanted parties (albeit at some risk of 'data breach fatigue' if they are not given practical response options).

Corporations that do not have in place strategic, comprehensive and reasonable data storage, location and jurisdiction policies, methodically and consistently adhered to in implementation, chance a fate serious in its potentially destructive outcomes, if the ire of judicial, regulator or market condemnation falls upon them. While many escape serious consequences (Telstra's recurrent large scale breaches come to mind), the risk of such condemnation remains.

What is cloud data?

Companies and individuals generate a plethora of digital documents, all of which are now candidates for, or generated by, cloud storage. For example:

- Images and recordings from mobile or other devices
- 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)
- Transaction records (including financial records)

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

- Other forms of meta-data
- Web pages (whether static or dynamically constituted)
- Traditional audio and video recordings and streams
- App data sets
- Software itself may constitute a significant cloud data holding
- Access control information and passwords

2. Types of Cloud Services

Different cloud models implement varied technical and processing attributes, and raise a range of different legal and policy issues around data sovereignty.

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.

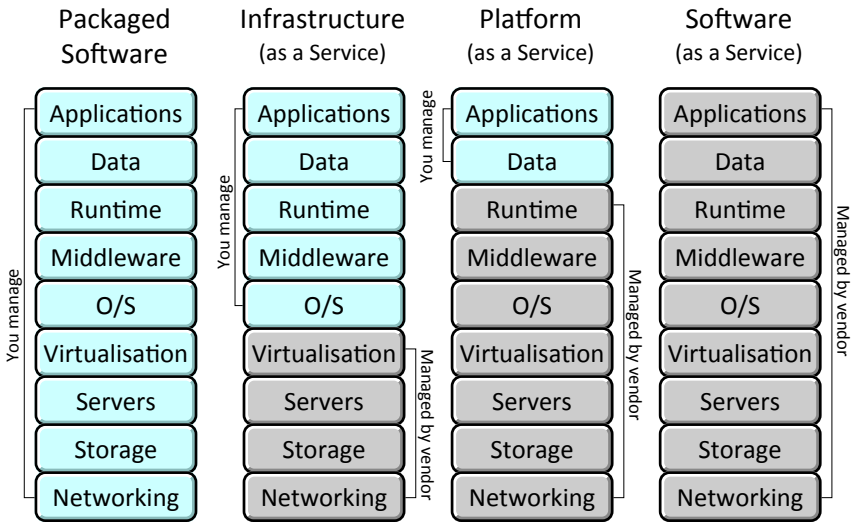

Figure 1. Cloud Service Models ***(Ludwig 2011, after Microsoft)*** [3]

Infrastructure as a Service (IaaS)

Here 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.

Platform as a Service (PaaS)

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

Interaction is medium when the cloud provider furnishes hosting and a platform, but not the specific applications running on it. This model is known as "Platform as a Service."(Gilbert 2010)

Software as a Service (SaaS)

The interaction may be large or frequent in "Software as a Service." The SaaS customer has access to a wide range of capabilities; the cloud provider furnishes hosting, storage, platform, as well as software applications for immediate use with the customer's data. Many consumer Cloud offerings like FaceBook, Google Docs, Apple iCloud or Microsoft OneDrive include core SaaS features.

Other Service Models?

Some commentators (Gilbert 2010) suggested other Cloud Service Models but the ones set out above appear to be a useful core set for most purposes.

Cloud Delivery Models

Cloud computing capabilities can be implemented and used in four main "Delivery models": Public, Private, Hybrid, and Community. The choice of delivery model has significant effect on the nature, content, and terms of the Cloud contract, and associated risks.

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. Most Amazon Web Services fall into this category, as do many offerings from Google, Facebook, Apple and Microsoft.

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-premises (presumably avoiding sovereignty or jurisdiction issues) or off-premises (which could be anywhere). It is more attractive to larger entities and government because of their greater capacity to manage their part of the investment and support required.[4] Many of these are not publicly visible, because they do not need to be.

Hybrid Cloud

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

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

between clouds. Many of the public cloud providers also offer private options, and can integrate the two. Data of different categories or sensitivity may thus be hosted in different delivery models, or indeed in different locations or under the control of different entities.

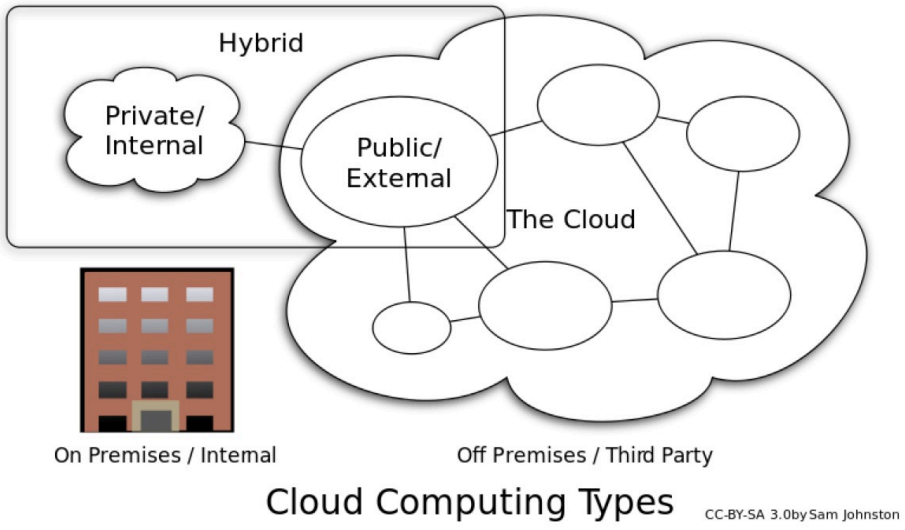

Figure 2 – Types of Cloud Computing [5]

Community Cloud

This approach is less common, typically used by government. A community cloud infrastructure is shared by several entities, supporting a 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 or off premises. (Gilbert 2010) Many government cloud installations are candidates for such a model.

Some features and risk attributes are shared by 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. Often by default it will be public Cloud delivery model, although off premises private clouds.

Real world: A mix of models and risks

The issues under consideration when we look at an actual Cloud implementation instance 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.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

- 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 analysis. Service and Delivery Models are a useful framework for this, 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 the Third Party Access section 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 may 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 may be higher or lower than if they were present, depending on configuration, contract and control details. (However, if the revelations in the documents leaked by whistleblower Edward Snowden are accurate, this risk is probably often higher than earlier appreciated, given the apparently omnivorous appetite for metadata surveillance by members of the 5 Eyes group, and possibly others.)

It is also useful to give close attention to the characteristics of the data, and the risks that different categories of data carry: only some classes of data are actually dangerous if lost. There is of course typically the embarrassment of a data breach: note the recent finding by ACMA against AAPT (ACMA 2013), the new penalties, and actual and proposed new disclosure obligations in the *Privacy Act 1988* (Cth)[6].

But it is also important to ask, how often is money or valuable data actually lost? The Verizon Data Breach Report (Verizon 2013) 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. (The Privacy Amendment (Privacy Alerts) Bill 2013,[7] the disclosures starting June 2013 (Greenwald 2013; Gellman and Poitras: 2013) and still continuing regarding secret NSA, GCHQ and related surveillance programs for data mining telecom and Internet providers, and the *Australian National Cloud Computing Strategy* (DBCDE: 2013)[8] combine to elevate cloud computing to the top of risk management considerations.)

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

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

the model, we turn now to the question of the exposure of data to third party access in the main Cloud hosting jurisdiction, the US.

3. 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.[9] 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. (It is worth noting the proposed secret TransPacific Partnership agreement reportedly appears to feature a specific provision prohibiting participants, such as Australia, from enshrining data location restrictions, and the equivalent Atlantic proposal includes similar constraints on domestic law. On the other hand the Article 29 Working Party has suggested that the EU consider restrictions; and they have been mooted by EU ministers and data protection commissioners post-Snowden.)

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

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

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. (Others may assume that 'industry practice' will suffice, and the OAIC *APP Guidelines*[10] of March 2014 tacitly accept a less restrictive approach. However ACMA's history of penalties suggests caution has a place.)

In some circumstances, this may mean that large categories of data should 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 above – where it cannot restrict the geographic location or jurisdictional control of its data, and where the characteristics of data warrant such caution.

In concept, using a public cloud on a multinational scale should be highly flexible and cost-effective for a business. One of the attractions is the promise of effectively outsourcing a range of costs and risks. However, t data sovereignty restrictions to which a company may need to adhere in relation to some of those risks can create 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 sections below on obligations and third party access.)

The Australian Experience

The new Australian Privacy Principles created by the 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," and there is greater expectation that the details of foreign jurisdictions in which personal data is hosted be disclosed

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

While there remains in the APP Guidelines (OAIC 2014) an emphasis on reasonableness, the new standard is potentially tighter, and the disclosure of diverse foreign locations hosting personal information of Australians potentially impacts reputation[11]. Thus, there may be an incentive to consider hosting in-country, or under a regime that is known to be even more rigorous and safe in practice than Australia's. In January 2013 it was 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, which have raise the bar for expectations of effective security in Australia (although it is too early to tell if this will eventuate, given the potential effect of other developments in the Snowden material raising questions about official involvement in moves to undermine security).

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, (Connolly and Vaile: 2012)[12] so evaluating the impact of cloud sovereignty issues in this context becomes difficult. Changes are due in 2014[13].)

Nevertheless, cloud computing is definitely on the rise in Australia. A recent study reported that more than half of the subset of Australian companies examined 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 (Frost and Sullivan 2012).

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 Australian Privacy Principles, which prohibit the transfer of personal information to a third party outside Australia unless that country has equivalent laws or the entity takes reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the information for the data (OAIC 2014, Chapter 8) [14]. Many state and territory privacy laws contain similar expectations.

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. (APRA 2010)[15]

Organizations in Australia, such as defence bodies, education providers, and healthcare organisations, may be required to adhere to the requirements of the Australian Government Information Management Office (AGIMO) to the extent they are directly acting for federal

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

agencies. AGIMO has set out issues to be considered by agencies that are exploring cloud services (AGIMO 2011) [16]. These agencies generally prefer to use data centres within Australia in order to maintain physical jurisdiction over their most sensitive data. (Many other activities of organisations other than federal agencies may not be required to adhere to AGIMO's guidance, depending on the nature of the contracts involved and of the organisation.)

Some cloud providers in Australia will commit to host services within national boundaries to alleviate these data sovereignty concerns. However, even if the data itself is hosted domestically, it is nonetheless conceivable that some service providing access to the data (for instance, in the case of certain models for offshoring by banks) 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.

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. (Irion 2012) (See also the Third Party Access section below.)

European Union

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 (Dekker 2012) [17] .

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 (EC Directorate-General for Justice 2012) [18] . If these proposals are implemented (Neilsen 2013), 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

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

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 (*Directive 95/46/EC*). 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, despite PATRIOT Act access and other emerging issues (Robinson 2013). (EU regulators and politicians appear to remain unmoved, with initiatives in the opposite direction in relation to 'Safe Harbor'.)

EU laws on 'discovery' for litigation purposes, and on national security, may be inconsistent with US laws such as the *USA Patriot Act* in some circumstances (Forsheit 2010). This may lead to confusion or conflict over appropriate responses to requests for access for this purpose.

USA

The United States has no overarching nationwide data protection law (HIPAA, though national, is restricted to the health sector), but it does regulate disclosure of certain categories of personal information to third parties through a variety of laws[19]. The US government asserts extraterritorial claims on data that potentially affect non-US entities through the *USA PATRIOT Act* [20]. These are discussed further in the next section.

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 personal information, to authorities [21] .

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 data store located within US boundaries. (See the SWIFT case below for an example on this point.)

There has efforts made to deal 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[22]. 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[23], among others.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

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 mounting criticisms of the effectiveness of Safe Harbor from a compliance perspective, including by UNSW research associate Chris Connolly. (Connolly 2008) These recently bore fruit in a review of trust schemes associated with it. (FTC 2014)

Data may also only be transmitted under the scheme to third parties who follow adequate data protection principles, thus obligating the cloud customer to ensure that its cloud provider operates responsively. Clearly there have been doubts about the effectiveness of this scheme; the Article 29 Working Party highlighted the question of whether individual/corporate consumers are in a position to understand (ie to give meaningful consent) and enforce such obligations.

More recently, EU concerns about the late 2013 revelations by Edward Snowden have brought the Safe Harbor model into question, given the apparently limited or non-existent constraints it has placed on warrantless suspicionless mass surveillance of non-US citizens. (Rodrigues et al 2013)

The European Parliament, after it adopted the text of the proposed EU General Data Protection Regulation on 12 March 2014, also went so far as to pass a resolution setting forth its findings and recommendations regarding the National Security Agency surveillance program. Among other things, the resolution calls for:

- withholding the Parliament's consent to the Transatlantic Trade and Investment Partnership if European data protection principles are not fully respected;
- suspending the Terrorist Finance Tracking Program until alleged breaches of the underlying data disclosure agreements have been fully clarified; and
- suspending the Safe Harbor Framework immediately, alleging it does not adequately protect European citizens. (Hunton & Williams 2014)

The long term future of the Safe Harbor scheme is thus unclear.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

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 within specific territories and provinces[24]. Of particular interest is Canada's assertion that its privacy laws apply beyond its borders. The Federal Court of Canada 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[25]. 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, though there are of course the sovereignty dilemmas around giving force to such powers.

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.

Data breach notification laws, for instance, vary greatly from one jurisdiction to the next. (Maurushat 2009) 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 cloud provider entity is subject to the laws of another country.

In addition, data which is transferred outside Australia to one or more 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 (Capgemini 2012).

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.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

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

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, 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 still subject to the laws of the jurisdictions where it is held, or which regulate entities who control or host it.

Data hosting customers need clarity about whether remote hosting will involve transferring data to a foreign legal environment that may bring new risks or create special concerns. 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

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

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 comparison of the substantive laws of the two 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. However, 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. These are of course to be offset against the hoped-for benefits of Cloud scale services.)

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).

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

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*. (BeVier 1999; Kisswani 2012)

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

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

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 article.

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[26], 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 consistent with perceived obligations under the Council of Europe Cybercrime Convention. It was opposed by industry, but returned to active consideration as the 2012 'Data Retention' proposals.

The Australian *Privacy Act* 1988 does not prevent a local company from providing 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. The concept of 'implied consent' has been used to justify provision where such statements are more ambiguous.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

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[27] to local data owners or individuals once personal data is disclosed as a result of foreign government or litigant compulsion or effective request. (Barwick 2012a)

There has, not surprisingly, been 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 now in force, while not requiring explicit consent, appear more likely under APP 8.1 and s 16C to impose liability on Australian hosts for data breaches which occur offshore in some circumstances. (See also the Privacy Alerts bill 2013, which would have imposed 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 (Cate 2007).

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).

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

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 (Cate 2007).

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[28]. 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[29];
2. the information on an individual's computer that was accessible by a peer-to-peer file sharing program[30];
3. the chat account information from Yahoo! of a person who used Yahoo's Internet services to access chat boards[31];
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[32]; and
5. the contents of an iTunes files library shared over an unsecured wireless network[33].

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[34].

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. (Roach 2010)

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*

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

(Interception and Access) Act 1979 (Cth). (Nicholls & Rowland 2007; Dobbie 2013)[35]."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[36].These bypass questions of 'reasonable expectation of privacy' with simple statutory exceptions, and the Privacy Commissioner's policy *Guidelines* to their use. (OAIC 2014) 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[37], 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"[38].

A reality check asking "who cares?" may however 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 is not 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 what 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

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

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[39].

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 (Lynch & Williams 2006).

In subsequent years further legislative changes have somewhat further reduced the difference between thresholds in the US and Australia (Michaelsen 2010), 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. More recent amendments have also broadened its use.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

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, 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[40]. 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[41]. 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[42]. 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[43].
4. The power to conduct roving wiretaps on communications lines, which allows for monitoring of several different communications lines across the US[44]. 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[45]. Third party communications carriers, landlords and other specified persons must provide access and assistance necessary to carry out the warrant[46]. They must not reveal the fact of the warrant, and must minimize associated disruption to any services they provide to the subject. In the

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

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[47]. 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[48].
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[49]. 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[50].

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. (Gellman & Poitris 2013) It was initially unclear the extent to which such programs, and the many others which followed, 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, (Greenwald & MacAskill 2013) 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[51]. 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 (Cate 2007). For example, nine NSLs in one investigation sought data on 11,100 separate telephone numbers

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

(Cate 2007). Moreover, a recipient of an NSL may not reveal its contents or even its existence[52].

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[53]. 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[54] 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 (Office of the Inspector General 2007).

(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[55]. 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 known 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 in by late 2013, and the Joint committee report declined to recommend it proceed. (JPCIS 2013) It is expected they would oblige increased retention so 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. There are however large numbers of warrantless metadata authorisations, over 300,000 in 2012-13, mostly by state police forces. (Attorney-General's Department 2012-13)

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

Reports in March 2014 suggest retention proponents remain enthusiastic. A Senate inquiry into the operation of the TIA Act, including this issue, is due to report in mid-2014, although with an unreceptive House of Representatives it appears unlikely its recommendations would be enthusiastically adopted.

The SWIFT case

A prominent example of the US government's use of an administrative subpoena is the SWIFT case. The 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 operated two primary data centres, an 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. (McNicholas 2009) 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[56] (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[57], 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

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

Directive 95/46/EC[58]). 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"[59]. 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. (McNicholas 2009) 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 (Salgado 2010).

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." (Beckwith Burr 2010) 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"[60].

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[61].

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"[62]. In contrast, the Ninth Circuit held that an electronic communication

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

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"[63]. 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[64].

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 (Salgado 2010).

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[65] is listed as an 'enforcement agency' under the *Telecommunications (Interception and Access) Act*.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

Also note the proposals for 'Data Retention', mentioned above, introduced publicly in 2012. 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)[66] contains two relevant provisions which offset the effect of prohibitions on phone tapping etc. under the *Telecommunications (Interception and Access) Act 1979* (Cth).[67] 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 ASIC IP block requests aimed at fraud pages reported to have inadvertently taken 1,200 and 253,00 non-fraud sites offline in two recent instances (LeMay 2013).

The more significant provision is an 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. Under s312 ACMA can issue administrative notices, also under an immunity; and the permissible scope for informal pressure on carriage service providers to 'do your best' under s313(1) and (2) is largely untested. The scope of these sections is thus somewhat uncertain, but clearly requires carrier help at least with reasonable law enforcement requests, including to assist 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[68].

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

Once the warrantless surveillance became known, 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[69].

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[70].

More recently discussions about the scope and oversight of NSA's PRISM and other programs, above, which came to notice in June 2013, were marked by difficulties experienced by members of Congress and 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, noted above. Although details and justifications of the proposal, which was mentioned briefly 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. 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, it 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.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

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 Cate & Eisenhauer 2007.

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" (Kessler et al 2008).

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

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

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's MSN, and America Online Inc., on the other hand, complied with the DOJ's request for both searches and addresses to varying degrees[71].

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"[72] (*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*[73]. 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 (Pryce 2006).

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

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

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*[74] (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[75]. 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*[76] 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.

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 (Citi Research 2012).

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.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

In considering the example of cloud data hosted in the United States, the differences between the legal environments in Australia and in the US 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 (although recent proposals may narrow the gap to some extent).

When the conduct of SWIFT in making its data available to the US Treasury 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." (European Parliament 2006)

While the potential for counterproductive "digital protectionism" deserves investigation, (Bleich 2012; Keane 2012) 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 (Walden & Luciano 2011) [77].

In our view, while the picture is complex, and examination of actual hazards and dangers may in some instances show limited exposure to risks worth caring about, the concerns expressed by the European Parliament 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.

5. A Signals Directorate view of Cloud security

Cloud services, with their massive 'honeypots' of tempting personal and business data and high capacity remote access, pose a serious challenge for IT security protection whether on shore or off, but they can also offer platforms for potentially meeting those threats in certain circumstances more effectively than non-cloud systems.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

A full exploration of Cloud security issues is beyond the scope of this paper, and will remain the subject of attention from a significant part of the IT security and research sector (Pavlotsky 2012; Srinivasan et al 2012) but we touch briefly on some of those related to jurisdiction and sovereignty, seen through the prism (pun intended) of the key Australian government security agency, what used to be called the Defence Signals Directorate. (DSD is now called Australian Signals Directorate.)

Cloud Computing Security Considerations – DSD Checklist

A non-exhaustive list of cloud computing security considerations is from section 17 of the Defence Signals Directorate/Cybersecurity Operations Centre, *Cloud Computing Security Considerations* (DSD 2012) [78] with cross references to other paragraphs for more information.

While companies and individuals may have a somewhat lower sensitivity to certain IT risks than some government agencies, 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 (Gold 2012) [79]. A cross beside any of these security considerations does not necessarily mean that cloud computing cannot be used, but the security consideration requires additional contemplation to determine if the associated risk is acceptable. The full list can be found in other works; items specifically relevant to data sovereignty questions include:

- My data or functionality to be moved to the cloud is not business critical (19a).
- 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).
- I retain legal ownership of my data (20i)
- Using the vendor's cloud does not weaken my network security posture (21b).
- The vendor does not know the password or key used to decrypt my data (22a).

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

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

contractually accept adhering to these obligations to help ensure 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 (DSD 2012, p10). Numerous reports in late 2013 have confirmed the frequent operation of such gag orders in the US, with some IT service providers but not others now campaigning for greater transparency. (Hill 2013)

These two issues may explain why DSD recommends agencies 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."* (DSD 2012, p1).

A notable feature is an apparent divergence by other agencies towards a more relaxed attitude to advice to the general public and business on Cloud data security, location and jurisdiction: while many operational federal agencies are anecdotally reputed to be still reluctant for security reasons to host their own key data off shore, some regulatory agencies appear more focused on promoting Cloud use for its own sake, with more limited explicit consideration of the jurisdiction aspects of security, and a tendency to focus on "benefits" alone rather than balancing benefits with costs, and in particular, risks (DoC 2014; AGIMO 2013; DBCDE 2013) [80].

If real, one explanation for this apparent inconsistency (if one assumes that underlying security and confidentiality needs are in fact similar) could be a conflict between industry development and free trade promotion considerations for the

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

broader public on the one hand, and security, privacy and confidentiality priorities for government data.

Such a conflict may explain the ambiguity in such divergent advice, and may also suggest a need for caution on the part of readers more attuned to the primacy of security, confidentiality and privacy.

6. Drivers for a Cloud Data Location and Jurisdiction Policy

This section provides an overview of the sorts of obligations or drivers to host Cloud data in one jurisdiction or another, and suggests one response to issues raised in the paper lies in an organisational policy on the topic. It also considers the special case of personal information, and the potential role of de-identification or the (newly controversial) US-EU Safe Harbor model in dealing with (or evading) constraints arising from privacy obligations.

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 refer to parallel or relevant European and US 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. (The proposed Trans-Pacific Partnership treaty has reputedly, in secret drafts shared with industry but kept from the public, promoted an alternative "digital protectionism" characterisation of jurisdiction-aware cloud contracts and may if implemented complicate the implementation of choices in this area. (Allgeier 2013, 4)

Cloud data location and jurisdiction policy

One response to challenges discussed in this paper and related material is a Cloud data location and jurisdiction policy, which can help guide the entire life cycle of all networked data within an organisation from creation to destruction. Such a policy would be founded on a survey of the specific requirements affecting each aspect of a business or agency. It could help answer questions about whether any data 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.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

Features of the organisation's regulatory environment such as the following can affect Cloud location and jurisdiction choices:

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

Factors affecting a Cloud Data Location and Jurisdiction Policy can include:

- The nature and security profile of the data (or sub-categories of it), and whether particular legal, regulatory or similar obligations favour certain locations or jurisdictions (Peterson et al 2011)
- The characteristics of 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 (Maxwell & Wolf 2012)

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

There are a number of reasons one 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

The second major reason for the local hosting of data is where you are *required by law* to retain the data in the local jurisdiction, or under the control of a entity regulated by that jurisdiction.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

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.

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); these are updated in the 2014 version (from the 2012 amendments).
- 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.

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.

It is important to note that, of course, many sorts of data are *not* however subject to any location-based statutory requirements, and can be stored off shore if this is consistent with other obligations and judgements.

Promises, promises: what you tell data subjects or providers at the point of collection

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

However, it is also 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 purposes. 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 or customers 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 its public (or, of course, to which it is bound in its contracts) when it decides to store data in the cloud in or under the influence of a certain jurisdiction. 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.

What data is regulated as "personal information"?

In contemplating criteria for assessing the security profile and hosting requirements of Cloud data (and hence the suitability of various jurisdictions), it is as we note above, important to consider detailed analysis of the application of particular provisions of applicable laws in relevant jurisdictions to certain classes of data, in addition to those relating to 'third party access' discussed elsewhere in this paper.

As noted above, a central concern is the nature of information considered to be "personal", and hence subject to privacy rules and other measures of sensitivity.

For instance "Personal information" (under Australian privacy law), "Personal Data" (EU) or "Personally Identifying Information" (US) refer to similar but not identical regulatory concepts for important data sets, ones that cover a relatively limited class of business information but often drive decision making.

It may be possible to ensure that information held by a service provider is de-identified and not easily re-identifiable. In such cases there are effectively no privacy rules applying to the data, since it is outside the 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.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

The revised *Privacy Act* in 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 paper from the US Department of Commerce (US Dept. of Commerce 2013) looks at a similar concept arising from the "Safe Harbor" 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.

However, as noted above, more recently various entities in Europe have, as result of the Snowden revelations, stepped back from the Safe Harbor arrangements, calling them into question. (European Parliament 2014)

7. Competing 'Frames': Digital Protectionism

Concerns raised by the revelations of Edward Snowden are reported to have already had a significant impact on the willingness of non-US business to adopt US based or controlled Cloud services without analysis of risks, with projected impacts running into the tens of billions of dollars over several years. (Hill 2013)

At the same time, there has been a concerted push to re-frame questions of Cloud location and jurisdiction as "digital protectionism", and thus an affront to free trade. (Snabe 2014; Young 2013)

For instance in its 2014 Report, "Powering the Digital Economy: A Trade Agenda to Drive Growth," (BSA 2014) the Business Software Alliance says:

"To spur trade in digital age products and services, BSA outlines a three-part agenda:

- First, modernize trade rules to reflect the realities of digital commerce as it is being conducted today. This requires facilitating trade in innovative services such as cloud computing, keeping borders open to the free flow of data, and preventing mandates on where servers or other computing infrastructure must be located.

- Second, promote the continued progress of technology innovation. For this, a trade agenda must secure modern intellectual property protections and encourage the use of voluntary, market-led technology standards.

- Third, create level playing fields for all competitors. That requires governments to lead by example. They should be fully transparent in how they choose which technologies to buy, basing decisions on whether a product or service best meets their needs and provides good value, not on where the technology was developed."

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

The controversial secret TransPacific Partnership (TPP) and Transatlantic Trade and Investment Partnership (TTIP, an Atlantic equivalent) also appear to have elements designed to implement this agenda: an industry lobbyist describes a key aim of the TPP as to "Prohibit parties from requiring the establishment or use of local servers or other infrastructure in order to provide digital products and services in a country" (Allgeier 2013, 4). (See also Assange 2013; US Trade Rep 2013)

This framing of the debate seeks to deprecate concerns over data location and sovereignty in the Cloud and other online services, just at the very time when these concerns are brought into dramatic relief by the controversial (and apparently ineffective) mass metadata and data surveillance practices revealed by Snowden. (Hill 2013)

It is perhaps ironic that the means (TPP and TTIP) of pursuing these clearly sectional interests are themselves challenged as being a threat to sovereignty, apparently even of the US, to the extent that they bypass normal democratic scrutiny (on the basis of being "merely about trade") yet purport to bind governments to implement national laws implementing rules negotiated in secret to tilt the playing field against those seeking to make jurisdictional choices about location and control of cloud data.

8. Conclusion

The bulk of the research for this paper occurred before the Snowden era, but the significant effects of Snowden's revelations about actual surveillance practices, and the threats to commercial and government cryptographic (Ball et al 2013) and other online security measures (Schneier 2013) represented by the 'security' agencies of Australia, the US, the UK and the other "5 Eyes" members have only tended to confirm the focus on third party access that forms a major part of this work.

The complex interlinking secret arrangements between the country that is home to much of the commercial Cloud, the US, and this country make legal and regulatory analysis difficult. There are certainly means to enable law enforcement and security cooperation between the two which tend to bypass locational and jurisdictional barriers. But there are also practical, legal and administrative effects of such barriers which are not wholly removed by such cooperation. On balance, for data which is significant and sensitive, there may still be benefits to considering location and jurisdiction issues.

In addition, the pressure for reform, not least from the two substantial reports by President Obama's hand-picked review team in December 2013 and the Congressional Oversight Board in February 2014, and court cases in the US (Judge Richard Leon, *Klayman and Strange v NSA*, US District Court for the District of Columbia in 16 December 2013) drawing out

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

concerns over lawfulness, proportionality and constitutionality, may over time rein in the excesses apparently revealed. The most disturbing of these relate to exceptional measures introduced to fight the exceptional perceived hazard of terrorism now being used for traditional international commercial trade espionage purposes (Jabour & Pengelly 2014).

If so, national sovereignty and jurisdiction over online data and metadata may regain something of its former significance.

It also remains to be seen if the agenda of US cloud and online business to deprecate data sovereignty concerns as unfair "protectionism", in spite of the apparently indiscriminate threats to online security and confidentiality revealed as sourced in their home jurisdiction, and to require national measures to restrict them is successfully implemented in the TPP and TTIP. If this were the case, exercising choices for consumers and business based on the perceived best location for security and privacy in the Cloud may be prevented or obstructed by law.

This would potentially reduce a significant incentive for all governments and businesses to respond to the Australian consumer preference for security and privacy of their data to be protected by location and jurisdiction measures, as identified by the survey which opened this paper. Personal information in particular, but government and business information as well, should probably be recognised as having critical risk characteristics beyond a status of mere trade commodities, such that their hosting in the Cloud may need to be open to whatever precautions and choices those liable for or subject to those risks may seek to make, including choices about location and jurisdiction. If these choices can be freely made, presumably the market will respond in creative ways, as indeed appears to be happening; were they to be constrained by law, the incentive for effectively addressing the concerns may be weakened, and the ultimate levels of trust and confidence in the cloud, the aim of good regulation, may be reduced.

Acknowledgements

This paper arises from a collaborative project (http://cyberlawcentre.org/data_sovereignty/) supported by NEXTDC (http://www.nextdc.com.au), Baker & McKenzie (http://www.bakernet.com) and AON (http://www.aon.com). Thanks to the following for their major contributions to earlier related works and this paper: Kevin Kalinich (AON), Patrick Fair and Adrian Lawrence (Baker and McKenzie); thanks also to Bruce Baer Arnold, University of Canberra, Alison Cook, postgraduate researcher, UNSW Law Faculty, Prof Graham Greenleaf, Professor of Law and Information Systems, UNSW Law Faculty, and interns including Tim Chiang, Annette Haddad, Natasha Hammond-Marks, Sasha Kolodkina, David Lee, Felix Lim, Lauren Loz, Peter Matuszak, Ryan Ruslim, Tia Singh, and

 http://doi.org/10.7790/ajtde.v2n1.31

Alice Yang (all of UNSW Law), and Cassandra Switaj (Bond University) and Bonnie Yiu (UTS). Responsibility is of course solely that of the author; project supporters and contributors to earlier related works may not necessarily endorse everything in this paper.

References

ACMA. 2013. 'AAPT warned about privacy', media release 26/2013, 24 April 2013. Available at: http://www.acma.gov.au/ theACMA/Newsroom/Newsroom/Media-releases/acma-issues-formal-warning-to-aapt

AGIMO. 2011. "Cloud Computing Strategic Direction Paper: Opportunities and for use by the Australian Government". April 2011. Available at: http://www.finance.gov.au/e-government/strategy-and-governance/cloud-computing.html

AGIMO. 2012. Better Practice Guide. (July 2012). 'Negotiating the cloud – legal issues in cloud computing agreements'. Available at: http://www.finance.gov.au/e-government/strategy-and-governance/ docs/negotiating_the_cloud_-_legal_issues_in_cloud_computing_agreements.pdf

AGIMO. 2013. "Australian Government Cloud Computing Policy: Maximising the Value of Cloud [for Australian Government Agencies]", Department of Finance and Deregulation, 29 May 2013. At: http://agimo.gov.au/files/2012/04/Australian-Government-Cloud-Computing-Policy-Version-2.0.pdf

Allgeier, P (President, Coalition of Services Industries (CSI)). 2013. "Services Business Objectives for TPP", U.S. Business Coalition for TPP, December 18, 2013, Available at: https://servicescoalition.org/images/TPP_Business_Coalition_Hill_Briefing_Dec_18_2013.pdf

APRA. 2010. Australian Prudential Regulation Authority (APRA) guidelines "Outsourcing and Offshoring: Specific considerations when using cloud computing services," 15 Nov. 2010, Available at: http://www.apra.gov.au/CrossIndustry/ Documents/Letter-on-outsourcing-and-offshoring-ADI-GI-LI-FINAL.pdf

Assange, J. 2013. US, Australia isolated in TPP negotiations, Wikileaks (editorial), 15th November 2013, Available at: http://wikileaks.org/US-Australia-isolated-in-TPP.html. Includes links to the IP chapter of the text.

Attorney Generals Department. 2013. *Telecommunications (Interception and Access) Act 1979 Annual Report*, 2012-2013, Available at: http://www.ag.gov.au/NationalSecurity/TelecommunicationsSurveillance/Documents/TSLB-GAPSTIAActAnnualReport2012-13.pdf

Ball, J; Borger J; Greenwald G. 2013. Revealed: how US and UK spy agencies defeat internet privacy and security, *Guardian Weekly*, 6 September 2013

Bamiah, MA; Brohi, SN. 2011. "Exploring the Cloud Deployment and Service Delivery Models", *International Journal of Research and Reviews in Information Sciences* (IJRRIS) Vol. 1, No. 3, September 2011, 77.

Barwick, Hamish. 2012a. 'The cloud security minefield', *CIO*, 5 September 2012.

Barwick, Hamish. 2012b. Data sovereignty still misunderstood in Australia: Microsoft,' *Computerworld*, 18 September 2012.

Baty, Craig. 2011. CTO, Fujitsu Australia and New Zealand, transcript of Korea-Australia-New Zealand (KANZ) Broadband Summit 2011. Available

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

at:http://www.archive.dbcde.gov.au/__data/assets/pdf_file/0005/138299/Craig_BatyCloud_Computing.pdf

BeVier, L. 1999. 'The Communications Assistance for Law Enforcement Act of 1994: A Surprising Sequel to the Break up of AT&T', *Stanford Law Review*, Vol. 51, No. 5 (May, 1999), pp. 1049-1125. http://dx.doi.org/10.2307/1229406. Available at: http://www.askcalea.net/

Bleich, Jeffrey (US ambassador). 2012. 'Cloud agreement can bring blue skies', The Age (Melbourne), 11 December 2012, Available at: http://www.theage.com.au/it-pro/government-it/cloud-agreement-can-bring-blue-skies-20121211-2b77f.html

Burr, J. Beckwith. 2010. *The Electronic Communications Privacy Act of 1986: Principles of Reform*, Available at <http://www.digitaldueprocess.org/files/DDP_Burr_Memo.pdf>.

Business Software Alliance. 2014. BSA Proposes Forward-Looking Trade Agenda to Stop the Spread of Digital Protectionism, 30 January 2014 Available at: http://www.bsa.org/news-and-events/news/2014/january/01302014digitaltradeagenda

Capgemini. 2012. "Business Cloud: The State of Play Shifts Rapidly: Fresh Insights into Cloud Adoption Trends," 29 November 2012, p.19, Available at: http://www.capgemini.com/business-cloud-the-state-of-play-shifts-rapidly/ or http://www.youtube.com/ watch?v=v_ga9orIzFI (worldwide survey of 460 IT and business leaders at companies with over 10,000 employees).

Cate, Fred H. 2007. 'The Vanishing Fourth Amendment', *Privacy and Security Law Report*, BNA, 6 *PVLR* 1875 (Dec. 10, 2007).

Cate, Fred H; Eisenhauer, Margaret P. 2007. Between a Rock and Hard Place: The Conflict Between European Data Protection Laws and U.S. Civil Litigation Document Production Requirements, 6 PVLR 229 (Feb. 5, 2007).

Chapman, Chris (Chair and CEO, ACMA). 2013. Opening remarks, Launch of 'Data Sovereignty and the Cloud—a Board and Executive Officers' Guide', 2 July 2013, Sydney. At: http://www.acma.gov.au/theACMA/Newsroom/Newsroom/Speeches/launch-of-data-sovereignty-and-the-cloud

Chawki, Dr Mohamed, Judge from the Egyptian Council of State. 2011. 'Egypt's Cyber Revolution: Tweeting from Tahrir Square', Cyberspace Law and Policy Centre, UNSW, 18 May 2011, at: http://cyberlawcentre.org/2011/talks/ltt_chawki.htm

Citi Research. 2012. *Cloud Computing – a two part series*, Part 2: Market Sizing, Barriers, Value Network and Outlook, December 2012, page 4.

Connolly, Chris. 2008. 'US safe harbor - fact or fiction?' *Privacy Laws and Business International* 96 December 2008.

Connolly, Chris; Vaile, D. 2012. Drowning in Codes of Conduct: An analysis of codes of conduct applying to online activity in Australia, UNSW Cyberspace Law and Policy Centre, March 2012, Available at: http://cyberlawcentre.org/onlinecodes/report.pdf

DBCDE. 2013. National_Cloud_Computing_Strategy 2013. Available at: http://www.dbcde.gov.au/__data/assets/pdf_file/0008/163844/2013-292_National_Cloud_Computing_Strategy_Accessible_FA.pdf

Dekker, M. 2012. *Critical Cloud Computing: A CIIP perspective on cloud computing services*, ENISA, December 2012. Available at: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/critical-cloud-computing/at_download/fullReport

Department of Communications (DoC). 2014. Cloud Computing Regulatory Stock Take, forthcoming, 2014 [after consultation in December].

Dobbie, Phil. 2013. 'Forget PRISM: Who's watching on your doorstep?', *SMH*, 18 June 2013, Available at: http://www.zdnet.com/au/forget-prism-whos-watching-on-your-doorstep-7000016935/.

DSD. 2012. Australian Signals Directorate. Cloud Computing Security Considerations. Available at: http://www.asd.gov.au/publications/csocprotect/cloud_computing_security_considerations.htm p1.

EC Directorate-General for Justice. 2012a. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21st Century*, COM/2012/09 final, 25 January 2012, Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52012DC0009:en:NOT

EC Directorate-General for Justice. 2012b. 'Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses,' media release, 25 February 2012, Available at: http://europa.eu/rapid/press-release_IP-12-46_en.htm

European Parliament. 1995. *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, Article 25, OJ L 281, 23.11.1995, Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:NOT

European Parliament. 2006. Resolution on the interception of bank transfer data from the SWIFT system by the US secret services, P6_TA (2006) 0317, 6 July 2006, Available at: http://www.europarl.europa.eu/sides/getDoc.do?Type=TA&Reference=P6-TA-2006-0317&language=EN

European Parliament. 2014. Resolution on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI) 21 February 2014, available at: http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&mode=XML&reference=A7-2014-0139&language=EN

Fleming, Jeremy 'US makes first public comment over draft EU data privacy law', *EurActiv*, 29 April 2013, at: http://www.euractiv.com/infosociety/us-airs-views-eu-privacy-rules-news-519279

Forsheit, Tanya L. 2010. "E-Discovery Involving Cloud Facilities." *Computer & Internet Lawyer* 27, no. 12 (December 2010): 1-7. *Business Source Premier*, EBSCOhost (accessed May 9, 2013).

Frost and Sullivan. 2012. *Australian Contact Centre Market* 2012, Available at: http://www.prnewswire.com/news-releases/frost--sullivan-cloud-based-contact-centre-solutions-poised-to-challenge-traditional-on-premise-model---growing-awareness-of-cloud-based-contact-centre-solutions-177556851.html; and http://www.mcafee.com/us/solutions/cloud-security/news/20120809-01.aspx

FTC. 2014. Federal Trade Commission. 'FTC Settles with Twelve Companies Falsely Claiming to Comply with International Safe Harbor Privacy Framework', Media Release, January 21, 2014, Available at: http://www.ftc.gov/news-events/press-releases/2014/01/ftc-settles-twelve-companies-falsely-claiming-comply

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

Gellman, B; Poitris, M. 2013. 'Documents: U.S. mining data from 9 leading Internet firms; companies deny knowledge', *Washington Post*, 7 June 2013, Available at: http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html. See Slides at: http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/

Gilbert, Francoise. 2010. 'Cloud Service Contracts May Be Fluffy: Selected Legal Issues to Consider Before Taking Off', *J Internet Law* 14 No. 6, December 2010, p 17

Gold, Joshua. 2012. 'Protection in the Cloud: Risk management and insurance for cloud computing' (2012) 15(3) *J Internet Law* 23

Greenwald, G. 2013. 'NSA collecting phone records of millions of Verizon customers daily', *The Guardian*, 6 June 2013, Available at: http://www.guardian.co.uk/world/2013/jun/06/nsa-phone-records-verizon-court-order

Hill, K. 2013. 'How the NSA Revelations are Hurting Businesses', *Forbes*, 10 September 2013, Available at: http://www.forbes.com/sites/kashmirhill/2013/09/10/how-the-nsa-revelations-are-hurting-businesses/

Hunton & Williams LLP. 2014. 'European Parliament Adopts Draft General Data Protection Regulation; Calls for Suspension of Safe Harbor', 12 March 2014, Available at: https://www.huntonprivacyblog.com/2014/03/articles/european-parliament-adopts-draft-general-data-protection-regulation-calls-suspension-safe-harbor/#more-5892

Irion, Kristina. 2012. 'Government Cloud Computing and the Policies of Data Sovereignty' (2012) 4 *Policy & Internet* 3, 40

Jabour, B; Pengelly, M. 2014. 'Australia spied on Indonesia talks with US law firm in 2013', theguardian.com, Sunday 16 February 2014, Available at: http://www.theguardian.com/world/2014/feb/16/australia-spied-indonesia-talks-us-firm

JPCIS. 2013. Joint Parliamentary Committee on Intelligence and Security (JPCIS). *Report of the Inquiry into Potential Reforms of National Security Legislation*, Parliament of Australia, 24 June 2013. At: http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/report.htm

Keane, B. 2012. 'Protectionism, free trade and security up in the cloud', *Crikey*, 12 December 2012, at: http://www.crikey.com.au/2012/12/12/protectionism-free-trade-and-security-up-in-the-cloud/

Kessler, David J; Coval, Christopher P; Blenkinsop, Peter. 2008. Is Personal Data Located Outside the United States 'Not Reasonably Discoverable'?, 7 *PVLR* 1356 (Sept. 15, 2008).

Kisswani, Nazzal. 2012."Telecommunications interception and access regulation framework in the US and the UK." *International Journal of Technology Policy and Law* 1, no. 1 (2012): 25-47. http://dx.doi.org/10.1504/IJTPL.2012.045944

Kuner, C. 2010. *Transborder Data Flow Regulation and Data Privacy Law* (Oxford: Oxford University Press, 2010)

Lee, Jane. 2012. 'Million-dollar fines set for privacy breaches', Sydney Morning Herald, 30 November 2012, Available at: http://www.smh.com.au/it-pro/security-it/milliondollar-fines-set-for-privacy-breaches-20121130-2al1e.html

LeMay, Renai. 2013. 'Interpol filter scope creep: ASIC ordering unilateral website blocks,' *Delimiter*, 15 May 2013, Available at: http://delimiter.com.au/2013/05/15/interpol-filter-scope-creep-asic-ordering-unilateral-website-blocks/

Ludwig, Sean. 2011. 'Cloud 101: What the heck do IaaS, PaaS and SaaS companies do?', *VentureBeat* blog, 14 November 2011, Available at: http://venturebeat.com/2011/11/14/cloud-iaas-paas-saas/

Lynch A; Williams, G. 2006. *What Price security? Taking Stock of Australia's Anti-Terrorism Laws* (2006) UNSW Press

Maurushat, Alana. 2009. 'Data Breach Notification Law Across the World from California to Australia,' *Privacy Law and Business International*, February 2009. Available as [2009] UNSWLRS 11 at: http://www.austlii.edu.au /au/journals/UNSWLRS/2009/11.html

Maxwell, Winston; Wolf, Christopher. 2012. 'A Global Reality: Governmental Access to Data in the Cloud – A comparative analysis of ten international jurisdictions (Governmental access to data stored in the Cloud, including cross-border access, exists in every jurisdiction)', Hogan Lovells, July 2012

McNicholas, Edward R. 2009.' National Security Letters: Practical Advice for Understanding and Handling Exceptional Requests' 8 *PVLR* 13 (Mar. 30, 2009). Available at http://www.sidley.com/publications/detail.aspx?pub=2047

Mayer-Schonberger, Viktor; Cukier, Keith. 2013. *Big Data, A revolution that will transform how we live, work and think* (John Murray/Hachette, London, 2013)

Michaelsen, Christopher. 2010. "Reforming Australia's National Security Laws: The Case for a Proportionality-Based Approach" (2010) 29(1) *University of Tasmania Law Review* 31

Morris, Chris/IDC. 2012. *Asia/Pacific (Excluding Japan) Cloud Services and Technologies End-User Survey, 2011*, IDC, November 2012.

Nicholls, R; Rowland, Michelle. 2007. "Message in a bottle: Stored communications interception as practised in Australia." In The Second Workshop on the Social Implications of National Security, p. 83. 2007

Nielsen, N. 2013. 'The man behind the EU Parliament's data regulation,' *EU Observer,* 6 May 2013, at: http://euobserver.com/justice/119951

OAIC. 2014. Office of the Australian Information Commissioner. *Guide to Handling Personal Information Security Breaches*. Available at: http://www.oaic.gov.au/publications/guidelines/privacy_guidance/Data_breach_notification_guide_April2012FINAL.pdf

Office of the Inspector General. 2007. *Report to Congress on Implementation of Section 1001 of the USA PATRIOT Act*, Mar. 2007. Available at <http://www.justice.gov/oig/special/s0703b/final.pdf

Office of the US Trade Representative, Trans-Pacific Partnership (TPP), 10 December 2013, http://www.ustr.gov/tppTR: 2013)

Pavolotsky, John. 2012. 'Cloud Services and Information Security: The Public vs. Private Service Provider Debate' (2012) 37 New Matter 1, 32, Available at: http://ssrn.com/abstract=2022519;

Peterson, Zachary N.J; Gondree, Mark; Beverly, Robert. 2011. 'A position paper on data sovereignty: The importance of geolocating data in the cloud', paper presented at Hotcloud 11, Portland, Oregon, USA, 14 June 2011. Available at: http://static.usenix.org/event/hotcloud11/tech/final_files/Peterson.pdf

Pryce, Jeffrey F. 2006. 'The Globalization of Electronic Evidence Gathering: U.S. Joins Council of Europe Convention on Cybercrime', 5 *PVLR* 1450 (Oct. 16, 2006).

QMUL Cloud Computing Project. 2010. 'What is Cloud Computing?', Queen Mary University London, 2010, Available at: http://www.cloudlegal.ccls.qmul.ac.uk/what/index.html

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

Roach K. 2010. 'The Eroding Distinction Between Intelligence and Evidence in Terrorism Investigations', in Andrew Lynch, Nicola McGarrity, George Williams, eds., *Counter-Terrorism and Beyond - The Culture of Law and Justice After 9/11*, Routledge, Sydney, May 2010.

Robinson, Frances. 2013. 'U.S. to EU: U.S. Data Law Is Brill,' *Wall Street Journal*, 19 April 2013, Available at: http://blogs.wsj.com/brussels/2013/04/19/u-s-to-eu-u-s-data-law-is-brill/.

Rodrigues, R; Barnard-Wills, D; Wright, D. 2013. 'EU privacy seals project: Inventory and analysis of privacy certification schemes', European Commission, Joint Research Centre, 2013.

Salgado, Richard. 2010. Written Testimony of Richard Salgado, Senior Counsel, Law Enforcement and Information Security, Google Inc., House Judiciary Subcommittee on the Constitution, Civil Rights and Civil Liberties, Hearing on *Electronic Communications Privacy Act* Reform (May 5, 2010).

Schneier, B. 2013. 'The US government has betrayed the internet. We need to take it back', *The Guardian*, Friday 6 September 2013

Snabe, Jim Hagemann. 2014. 'Don't let data protection turn into protectionism' Reuters US - Opinion: The Great Debate, 9 January 2014, Available at <http://blogs.reuters.com/great-debate/2014/01/09/dont-let-data-protection-turn-into-protectionism/>.

Srinivasan, Madhan Kumar; Sarukesi, K; Rodrigues, Paul; Sai Manoj, M; Revathy P. 2012. 'State-of-the-art cloud computing security taxonomies: a classification of security challenges in the present cloud computing environment', International Conference on Advances in Computing, Communications and Informatics, Chenai, India, 5 August 2012

Svantesson, D J. 2013. *Extraterritoriality in Data Protection Law* (Copenhagen: Ex Tuto, 2013)

US Dept. of Commerce. 2013. 'Clarifications Regarding the US EU Safe Harbor Framework and Cloud computing', April 2013. Available at: http://export.gov/static/Safe%20Harbor%20and%20Cloud%20Computing%20Clarification_April%2012%202013_Latest_eg_main_060351.pdf

Verizon. 2013. 2013 *Data Breach Investigations Report*. Available at: http://www.verizonenterprise.com/DBIR/2013/

Walden, Ian; Luciano, Laise Da Correggio. 2011. 'Ensuring Competition in the Clouds: The Role of Competition Law?' (April 7, 2011), Available at http://ssrn.com/abstract=1840547

Young, Michael. 2013. 'Global Protectionism on the Rise - But who's being protected? Citizens or local competitors?' *Tech Page One*, 23 December 2013 Available at <http://techpageone.dell.com/business/global-protectionism-rise/#.UvxKAL9WjHg>.

Zimmerman, M. 2013. 'In Depth: The District Court's Remarkable Order Striking Down the NSL Statute', EFF, 18 March 2013, Available at: https://www.eff.org/deeplinks/2013/03/depth-judge-illstons-remarkable-order-striking-down-nsl-statute

---

[1] Co-convenor, Cyberspace Law and Policy Community, UNSW Faculty of Law, d.vaile@unsw.edu.au.

[2] See for instance the government and corporate strategy documents listed in our extensive bibliography published last year in this journal.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

[3] Based on material from Microsoft, 'Windows Azure Platform: Cloud Development Jump Start' via podcast at http://itunes.apple.com/si/podcast/windows-azure-platform-cloud/id415763483, in Ludwig 2011

[4] Private cloud users do not raise loss of control and security as much: see Morris/IDC 2012.

[5] Image from Sam Johnston at: http://en.wikipedia.org/wiki/File:Cloud_computing_types.svg.

[6] Australian Privacy Principles in force from 14 March 2014 encourage greater disclosure of countries to which personal information may be sent. The proposals from ALRC and Prime Minister and Cabinet leading to the 2013 breach notification "privacy alerts" bill lapsed with the 2013 election.

[7] The Privacy Amendment (Privacy Alerts) Bill, introduced to Federal Parliament on May 29, 2013, would have amended the *Privacy Act* 1988 (Cth) (*Privacy Act*) to require data breach reporting obligations for a "Serious Breach" for entities regulated by the Privacy Act, making it less likely an Australian cloud provider could avoid revealing personal info data breaches for personal info under their control -- wherever it is held. A serious data breach is where an Australian entity holds personal information relating to one or more individuals, and the information is either: (a) accessed or disclosed without authority, and the access or disclosure will result in a "real risk" of serious harm (including financial or economic harm and harm to reputation); or (b) lost in circumstances where (a) may occur. A serious data breach also occurs where an overseas entity holds personal information that has been disclosed to it by an Australian entity in accordance with Australian Privacy Principle 8.1, and (a) or (b) occurs in respect of that foreign entity. Where a breach reporting obligation arises, the entity must prepare a disclosure notice setting out the nature of the data breach, information at risk, and any steps that affected individuals can take to mitigate the effects of the breach. Failure to notify the Commissioner or affected individuals when required to would be an "interference of the privacy of an individual". This would have triggered enforcement rights under the *Privacy Act*, including the possibility of a determination by the Commissioner that the entity is required to pay compensation to affected individuals and can also attract a civil penalty of up to $1.7million for corporations. Exemptions would have reduced the impact. Given pressure from jurisdictions in US and EU with such laws already in place, a revised version of these requirements may eventually return to Parliament.

[8] See http://www.dbcde.gov.au/__data/assets/pdf_file/0008/163844/2013-292_National_Cloud_Computing_Strategy_Accessible_FA.pdf

[9] For an extreme example, the then Egyptian government suspended internet services in the Arab spring of 2011 by the simple but [technically if not politically!] effective expedient of blocking access to the key packet routing infrastructure, both internally and out of the country, for a short period, for all but a tiny group of government networks. See Dr Mohamed Chawki 2011

[10] OAIC At: http://www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/

[11] Though note observations by Nigel Waters, Australian Privacy Foundation policy committee chair and former deputy Privacy Commissioner, who suggests the new law weakens, rather than strengthens privacy protections because it does not give people the right to have a complaint determination made, noting the Privacy Commissioner's office has made only nine determinations in 23 years. "This approach assumes the Australian government is in a position to do something about breaches that occur in another country. At the end of the day the only redress is if the company decides to bring a civil proceeding against [a party in] the country, which is nowhere near as effective as an individual being able to complain directly about the breach." Lee 2012

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

[12] For an analysis of Code complexity, see Chris Connolly and D Vaile 2012

[13] The *Privacy Amendment (Enhancing Privacy Protection) Act* 2012 (Cth) becomes effective in March 2014, with penalties of up to $1.1 million. Before then, different rules applied for private businesses and the public sector; there is still no state or federal statutory tort or similar cause of action for invasion of privacy; and in many other ways Australia's information security laws fall short of international best practice standards. In particular, Australia has lagged behind foreign counterparts in enacting laws holding businesses responsible for losing sensitive information about their customers, employees, and others. Organisations may voluntarily report security breaches, but very few do. Australian does not impose any binding general obligation to do so except in limited circumstances, such as the *Personally Controlled Electronic Health Records Act* 2012 provisions requiring notification if unauthorized disclosure of patient health information has occurred; see Part 4, at: http://www.comlaw.gov.au/Details/C2012A00063/ Html/ Text#_Toc327957207. For the most part though, breach notification is voluntary, and businesses are encouraged to use the Office of the Australian Information Commissioner's *Guide to Handling Personal Information Security Breaches*, at: http://www.oaic.gov.au/publications/guidelines/privacy_guidance/Data_breach_notification_guide_April2012FINAL.pdf. A voluntary scheme with unenforced compliance may offer perverse incentives to avoid compliance, especially where voluntary notifiers have no protection and fear being singled out for publicity. (The 2013 Privacy Alerts bill, which may strengthen reporting obligations, is covered below.)

[14] See also s 16C *Privacy Act*, which holds the disclosing entity accountable for any acts or practices of the overseas recipient in relation to the information that would breach the APPs.

[15] APRA, the Australian regulatory authority overseeing Australian banks, determines whether they may use public cloud computing that hosts data offshore on a case-by-case basis. Although there are no laws explicitly prohibiting a bank from using an offshore cloud provider, APRA's outsourcing risk management guidelines make it difficult for banks to enter in to such arrangements as a practical matter. APRA requires banks to obtain preapproval to use offshore data centres by showing the existence of adequate risk management procedures. Banks must also elicit from the vendor a contractual commitment to allow APRA access to the data centre. Some banks have aggressively pursued cloud solutions, even public offshore clouds, but with a measure of trepidation due to regulatory uncertainty. Like banks, insurance companies must also obtain APRA approval to use cloud environments hosted outside Australia's borders or jurisdiction.

[16] See also "Negotiating the cloud – legal issues in cloud computing agreements: Better Practice Guide" (July 2012), http://www.finance.gov.au/e-government/strategy-and-governance/ docs/negotiating_the_cloud_-_legal_issues_in_cloud_computing_agreements.pdf

[17] "From a security perspective, the concentration of data is a 'double-edged sword'; large providers can offer state-of-the-art security, and business continuity, spreading the costs across many customers. But if an outage or security breach occurs, the impact is bigger, affecting many organisations and citizens at once." See Dekker 2012

[18] For the proposal, see EC Directorate-General for Justice, 25 January 2012. See section 4., 'Data protection in a globalised world', for impact on hosting EU data outside EU. For a summary, see EC Directorate-General for Justice, 25 February 2012

[19] See section 4, "*Third party access by legal means: Does it matter where your data is stored?*" For instance, health information may not be transferred to a service provider unless that provider agrees to comply with the *Health Insurance Portability and Accountability Act* (HIPAA). The *Violence Against Women Act* prohibits domestic violence service providers from disclosing information to third parties without consent. (Public Law

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

109-162 as amended by Public Law 109-271). Income tax return information may not be disclosed without the taxpayer's consent. (*Internal Revenue Service Rules* - 26 U.S.C. § 6713 and § 7216; 26 C.F.R. §301.7216) A financial institution may not disclose personal financial information about a consumer without his or her consent: The *Gramm-Leach-Bliley Act* (15 U.S.C. § 6802); Video and cable television records may not be disclosed. *Video Privacy Protection Act* (18 U.S.C. § 2710) and *Cable Communications Policy Act* (47 U.S.C. § 551).

[20] *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism* (*USA PATRIOT Act*) of 2001, at: http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/html/PLAW-107publ56.htm

[21] The *PATRIOT Act* permits the US government to obtain personal information held in any country in the world that is being held by US companies, or those with sufficient connections to the US. The US Federal Bureau of Investigation (FBI) may obtain a court order requiring US Internet service providers to disclose records stored on their servers, without the data subject even being notified. Thus, if cloud data is transmitted to the US or merely hosted by a US-based company anywhere in the world, it is potentially subject to the *PATRIOT Act*. See section 4 below.

[22] US-EU Safe Harbor, 2000, at: http://export.gov/safeharbor/eu/eg_main_018365.asp

[23] US-Swiss Safe Harbor, 2008, at: http://export.gov/safeharbor/swiss/index.asp

[24] Canada's national "Personal Information Protection and Electronic Documents Act" (PIPEDA) regulates personal data gathered and maintained in the course of commercial activities. PIPEDA requires advance consent for disclosure of personal information and must allow individuals to correct inaccurate information. Provincial laws in Alberta, British Columbia, and Quebec offer additional privacy protection similar to PIPEDA, but each has its own definition of "personal data."

[25] *Lawson v. Accusearch Inc.*, (F.C.), 2007 FC 125, [2007] 4 F.C.R. 314, February 5, 2007, Docket:T-2228-05, at: http://reports.fja.gc.ca/eng/2007/2007fc125/2007fc125.html

[26] *See* Digital Due Process, at: http://www.digitaldueprocess.com/

[27] While Australian Law Reform Commission recommended (see Chapter 31 of *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008) that privacy laws should provide that an agency or organisation that transfers personal information about an individual outside Australia will remain responsible for the protection of that information, in the hope of ensuring that an individual has the ability to approach a local privacy regulator and seek redress from someone in Australia if the overseas recipient breaches the individual's privacy, this responsibility was excluded if the entity was 'required or authorised by law' to transfer it. Recent amendments to the *Privacy Act*, discussed above, partly strengthen this exclusion by basing the new test on compliance with Australian law. Similar exceptions would be expected in the event of disclosure to third parties where this is 'required or authorised by law'. ALRC suggested merely that the Privacy Commissioner should offer 'guidance' to transferors, recommending 'a warning that foreign laws might require the disclosure of the information to foreign government agencies'. <http://www.austlii.edu.au/au/other/alrc/publications/reports/108/31.html#Heading748>

[28] Tenth Circuit Finds no Expectation of Privacy in Data Given Freely to ISP, 7 *PVLR* 418 (Mar. 24, 2008).

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

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

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

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

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

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

[34] *Lukowski v. County of Seneca*, W.D.N.Y., No. 08-CV-6098 (Feb. 24, 2009); Privacy Interest in ISP-Stored Identifying Data Held to Depend on Terms of Service, 8 *PVLR* 397 (Mar. 9, 2009).

[35] Detailed statistics are provided in Attorney Generals Department, *Telecommunications (Interception and Access) Act 1979 Annual Report*, 2012-2013, at: http://www.ag.gov.au/NationalSecurity/TelecommunicationsSurveillance/Documents/TSLB-GAPSTIAActAnnualReport2012-13.pdf

[36] Exceptions 10.1(d) and 11.1(e) were part of the Information Privacy Principles which bind federal agencies prior to the December 2012 amendments coming into force in 2014; there were similar provisions in the National Privacy Principles which apply more broadly, and in the new Australian Privacy Principles. They prevent use beyond that for which it was collected or consented to [unless] 'use of the information for that other purpose is reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue.'

[37] Pub. L. 95-511

[38] ACLU Challenges FBI National Security Letter; First Use of Power to Demand Library Data, 4 *PVLR* 1105 (Sept. 5, 2005).

[39] *See* http://www.ag.gov.au/agd/www/nationalsecurity.nsf/AllDocs/85A16ADB86A23AD1CA256FC600072E6B? OpenDocument, revised 2005.

[40] 50 U.S.C. § 1861(a)(1); Section 215 of the *USA Patriot Act* of 2001 amended *Foreign Intelligence Surveillance Act*. Code section references in footnotes below are to the relevant sections of *FISA* as amended by Section 215 of *USA Patriot Act*.

[41] 50 U.S.C. § 1861(c) <http://www.law.cornell.edu/uscode/html/uscode50/usc_sec_50_00001861----000-.html>

[42] 50 U.S.C. § 1822(a)(1) & (4) <http://www.law.cornell.edu/uscode/html/uscode50/usc_sec_50_00001822----000-.html>

[43] 18 U.S.C. § 3103a(c) <http://www.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00003103---a000-.html>

[44] 50 U.S.C. § 1805(c)(3) <http://www.law.cornell.edu/uscode/50/usc_sec_50_00001805----000-.html>

[45] 50 U.S.C. § 1805(a)(2); as above.

[46] 50 U.S.C. § 1805(c)(2)(B) ; as above.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

[47] 50 U.S.C. § 1802 <http://www.law.cornell.edu/uscode/50/usc_sec_50_00001802----000-.html>

[48] 50 U.S.C. § 1802(a)(4) ; as above.

[49] 50 U.S.C. § 1842 <http://www.law.cornell.edu/uscode/50/usc_sec_50_00001842----000-.html>

[50] 50 U.S.C. § 1842 (c)(B)(i)-(ii) ; as above.

[51] 'High Court Pick Sotomayor Ruled for ISP in National Security Letter Free Speech Case', 8 *PVLR* 808 (June 1, 2009).

[52] *High Court Pick Sotomayor Ruled for ISP in National Security Letter Free Speech Case*, 8 PVLR 808, June 1, 2009

[53] See *National Security Letter Statute* (18 U.S.C. § 2709) at: <http://www.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00002709----000-.html>

[54] *John Doe Inc., et al. v. Mukasey, et al.,* US CA 2nd Circuit NY, Docket 07-4943-cv, December 15, 2008, at: http://www.aclu.org/pdfs/safefree/doevmukasey_decision.pdf

[55] *In re National Security Letter,* Docket C 11-02173 SI, US DC Northern District California, Order Granting Petition to Set Aside NSL, 15 March 2013, at https://www.eff.org/node/73523. See also Zimmerman M, 18 March 2013

[56] See < http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm>

[57] Personal communication to co-author from senior SWIFT officers visiting UNSW in 2008.

[58] EU Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; OJ L 281, 23.11.1995, p. 31–50).

[59] <http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/07/266>

[60] Recent Lawsuit Shows Challenges in Applying Warrant Rule, SCA to Remotely Stored E-Mail, 9 *PVLR* 618 (Apr. 26, 2010).

[61] *Id*.

[62] *Rehberg v. Paulk*, No. 09-1187, 11th Cir. (Mar. 11, 2010).

[63] *Quon v. Arch Wireless*, 529 F.3d 892 (9th Cir. 2008).

[64] *Warshak v U.S.*, 490 F.3d 455 (6th Cir. 2007).

[65] CrimTrac is a Commonwealth government organization designed to assist law enforcement by creating databases and coordinating national information sharing solutions; it has no direct law enforcement role.

[66] At: http://www.austlii.edu.au/au/legis/cth/consol_act/ta1997214/s313.html

[67] At: http://www.austlii.edu.au/au/legis/cth/consol_act/taaa1979410/

[68] Privacy Groups Urge Democrats to Review Bush Anti-Terror Programs, 6 *PVLR* 132 (Jan. 22, 2007).

[69] House Approves FISA Reauthorization bill with Retroactive Telecom Immunity Provision, 7 *PVLR* 931 (June 23, 2008); Bush Signs Wiretap Law, which Lacks Retroactive Liability Protection for Companies, 6 *PVLR* 1279 (Aug. 13, 2007).

[70] Anti-Terror Issues Could Drive New Surveillance Privacy Rules, 8 *PVLR* 59 (Jan. 12, 2009).

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

[71] *Gonzales v. Google, Inc.*, 234 F.R.D. 674 (N.D.Cal, 2006), < http://www.google.com/press/images/ruling_20060317.pdf>; Judge Orders Google to Surrender to DOJ 50,000 Random Internet Addresses, 5 *PVLR* 437 (Mar. 27, 2006).

[72] *In re Uranium Antitrust Litigation*, 480 F. Supp. 1138, 1144 (N.D. Ill. 1979) (distinguishing from the situation where a US court orders someone in the US to produce documents located abroad).

[73] Subject to reservations retaining the operation of existing bilateral mutual assistance treaties and US law in some respects. *See* http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG

[74] *Treaty between the Government of Australia and the Government of the United States of America on Mutual Assistance in Criminal Matters, and Exchange of Notes,* [1999] ATS 19, <http://www.austlii.edu.au/au/other/dfat/treaties/1999/19.html>

[75] *See* <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG>

[76] Legislation implementing the *Convention* passed in 2012 and it came into force in Australia in March 2013.

[77] While pre-dating emerging protectionism debates, Walden &Luciano suggest that alternative legal mechanisms, specifically measures to promote open standards and interoperability in the context of public procurement, as well as a data portability right as a demand-side measure, are likely to have a more significant impact on competition in the cloud computing sector than intervention using traditional competition measures. More recently, see Swedish Data Inspection Board's decision of 10 June 2013 against the use of certain cloud apps by public sector body due to contractual uncertainty, at: http://www.datainspektionen.se/press/nyheter/2013/fortsatt-nej-for-kommun-att-anvanda-molntjanst/; see also http://www.privacysurgeon.org/blog/incision/swedens-data-protection-authority-bans-google-apps/.

[78] DSD DSD: 2012/Dept. of Defence, Canberra, September 2012. At: http://www.dsd.gov.au/infosec/cloudsecurity.htm

[79] See also section 3 above

[80] Others see bibliography; Department of Communications (DoC), Cloud Computing Regulatory Stock Take, forthcoming, 2014

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31

Cite this article as: Vaile, David. 2014. 'The Cloud and Data Sovereignty after Snowden'. *Australian Journal of Telecommunications and the Digital Economy* 2 (1): 31.1-31.58. DOI: http://doi.org/10.7790/ajtde.v2n1.31. Available from: http://telsoc.org/journal

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n1.31